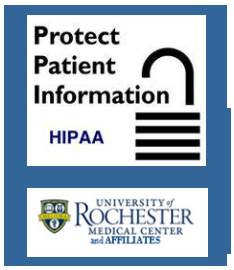
HIPAA HIGHLIGHTS

December 2021



Important Reminders: Verifying You Have the Correct Patient / ⃠ Snooping

Paper document errors **are the most frequent HIPAA breaches of PHI at URMC and Affiliates,** and they highlight the enormous responsibility of handling patient information. Examples include AVSs, lab results, lab requisitions, medications, itemized bills, statements of payment, referrals, and appointment and other letters. When misplaced or given out to the wrong patient, commonly used documents can have serious implications for the patient and our organization. Follow a standard process when managing these documents.

The **Patient Document Handoff Standard** outlines steps for in-person handoffs of paper documents that if followed, greatly reduce the chance of giving PHI to the wrong patient. Some steps are adaptable to mailed documents as well. These steps include:

- Always greet the patient upon entry & exit and obtain two patient identifiers, usually Name and Date of Birth.
- Ask patients with MyChart that do not require post procedure instructions if they would like to receive their AVS via their MyChart. If they agree, **you do not need to print** the AVS.
- Do not hand-off separate documents to the patient. Wait until all of the documents they require have been printed.
  - Do not staple or clip the documents together;
  - Do not place them underneath an object or other non-PHI documents.
- Always review each printed page for the two patient identifiers:
  - Highlight the identifiers if this is part of your department process.
- Always make eye contact with the patient during the handoff process. Involve the patient in the process. Ask them to review each page for accuracy of their demographics. If an error has been made, this is the time to correct it, not after the patient has left the area!

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.

If accessing a patient's record is not required by your job function, the access is NOT allowed! If there is a need for a patient's family member to have access to patient care information, consider alternatives such as the MyChart Proxy.

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 patient complaint or through "whistleblower" calls from workforce members.

Snooping in the patient record could terminate your employment or result in the loss of privileges. 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.

Snooping is a HIPAA Privacy breach. When an unauthorized access or disclosure occurs, the Privacy Office determines whether the patient needs to be notified per HIPAA Policy 31.

Remember, patients rely on us to protect their information! You hold the key to making sure that happens!

For additional information on any HIPAA-related topics, please refer to the URMS intranet site at http://sites.mc.rochester.edu/departments/hipaa/ . For any questions regarding HIPAA, please contact your Privacy Officer or HIPAA Security Official.