HIPAA

Health Insurance Portability & Accountability Act

- **Use and/or disclosure of PHI**
  - Remember the use and disclosure of PHI must be limited to the minimum necessary to accomplish the intended purpose. Ask yourself if it is in the best interests of the patient before using or disclosing; always document your reasoning.
  - ***Use*** means using PHI within an entity that holds such information (within our "four walls")
  - ***Disclosure*** means the release, transfer, access, or divulging PHI outside the entity holding such information (outside our "four walls")
- **Protection of PHI**
  - Do not leave PHI accessible; know where your documents are going (printing, emails, fax, etc.)
  - Place all confidential papers including those with PHI in the designated confidential Shred Bins when you no longer need the papers.
- **Access to PHI**
  - If access is not needed for your job, don't access PHI. 'Snooping' in patient medical records is never ok.
  - Looking at your own records or your family and friends' records is **prohibited**.
  - Never share your passwords or login credentials; log off or secure your computer workstation when its unattended or at the end of the day.

Remember…

- **Minimize incidental disclosures of PHI**. Be aware of those around you when discussing PHI. Sounds tend to carry, and others might overhear discussions taking place. Avoid conversations in non-secure areas like hallways, elevators, or the cafeteria. Be mindful of your tone and volume. Only discuss PHI with those who have a ‘need to know’.

Remember…

- **Disposal of PHI** - If a document has confidential patient information (personal and/or healthcare related) on it, it must be shredded when you are completely done with it - this also includes other miscellaneous types of documents that contain patient information such as patient labels, armbands, etc.

- **Control your workspace.** Take time to ensure your work area is secure before you leave it. Documents should not be left on shelves, desks, or counter tops that cannot be secured. Always keep PHI out of sight and secure it when not in use. You are responsible for keeping the patient information you always work with confidential.

Remember…

- **“Lock Before you Walk”** When you step away from your computer, it is not enough to just minimize what is on the screen. Lock your workstation to prevent others from using your computer when you are away from your desk. (ctrl+alt+delete or the windows logo key + “L”) You are responsible for all action and accesses under your login credentials.

- Not taking precautions to protect computer screens from prying eyes can be a HIPAA violation. Computer screens and other devices that display patient information should be positioned in a way that prevents exposure of PHI to others.

Remember…

- **Be Social, Stay Compliant.** Never post about patients, their information or details of any situation on any Social Media platform. EVER. Not even in broad, general terms or when names aren't used. Even if you think you're being subtle, you're not. Keep your professional and personal lives separate.
- **Never** take pictures or post pictures of patients on social media and never interact with posts that a patient makes about their own medical situation.
- **Text-Messaging** or instant messaging of PHI on cell phones whether personally owned or provided by Mon Health is **prohibited**.

Remember…

- Any use or disclosure of PHI without the patient's authorization or outside of Treatment, Payment or Operations (TPO) is considered a **Breach**.
- **Early Reporting** of potential Breaches is key to limiting the potential impact of a privacy or security incident and resolving the situation.
- If you observe or become aware of a HIPAA violation, incident or issue it must be reported to:
  - Your Direct Manager or Supervisor (who will report it to the System Privacy Officer)
  - Lauran Gregory, System Privacy Officer – 304-285-2204 or privacy@monhealthsys.org
  - ComplianceLine Hotline – 844-536-3273