HIPAA Privacy & Security: What You Need to Know

Providence St. Joseph Health (PSJH) expects that all workforce members and those with access to our electronic health records will protect our patients' information in accordance with the HIPAA privacy and security rules and applicable state laws. This tip sheet highlights key HIPAA focus areas. In a time of increasing government enforcement, fines and potential jail time, these tips will help you do the right thing.

- *Never* view patient records outside your scope of work. Only view records relevant to performing you job. **No snooping!**
- *Never* share your ID or passwords with anyone and do not allow others to use the computer while you are logged in. Don't leave your password written down near your computer. Make certain to lock or log off your computer when you step away.
- Understand what qualifies as **protected health information (PHI).** **Some** examples of PHI include:

  - Names and addresses
  - Telephone/Fax Numbers
  - Email Addresses
  - Social Security Numbers
  - Medical Record Numbers
  - Dates that include Dates of Birth, Death, Admission, Discharge
  - Full-Face Photos and Comparable Images of Patients
- Use secure shredder bins to dispose of documents containing PHI or other confidential information. Never trash documents containing confidential information.
- Keep PHI out of sight and secure it when not in use to prevent unauthorized access.
- Avoid patient-related discussions in public areas.
- You are responsible for keeping health information received at work confidential. Do not post PHI to social networking sites such as Facebook, Instagram, Snapchat, etc. This is a serious HIPAA violation and constitutes a breach.

- Always use a cover sheet when transmitting information by fax. Do not put confidential information on the cover sheet.
- Before discarding pill bottles, IV bags, vials or other items with labels containing PHI, black out the information or remove the labels and dispose of them in the shredder bin.

- Understand what constitutes a breach. A **breach** is defined as the impermissible acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the information. Healthcare professionals that violate privacy laws and regulations, and commit a breach can face very serious consequences. These can include progressive discipline, up to and including termination. Healthcare professionals may also face criminal prosecution and civil penalties up to $250,000. The best way to prevent a breach is to always keep the information obtained at work confidential and follow proper security practices when dealing with PHI.

- Examples of potential breaches include:
    - Viewing patient records without the "need to know"
    - Throwing PHI in the trashcan instead of the shredder bin
    - Giving discharge summaries and prescriptions to the wrong patient
    - Posting patient information/PHI to social networking sites or blogs
    - Sending faxes with confidential information to the wrong recipient
- Understand how to report a compliance issue or suspected breach:

    1. Discuss the issue or concern with your immediate supervisor
    2. Discuss the issue or concern with the department manager
    3. Contact your Regional Privacy Officer at 806-725-1307
    4. Enter an Integrity Hotline report through EthicsPoint.
    5. Call the Providence Integrity line at (888)294-8455. The Integrity Line is available toll- free 24 hours a day, 7 days a week. You may report concerns anonymously.

- Consult PSJH Code of Conduct when you have questions about doing the right thing. The Code will help you understand PSJH expectations and the importance of being honest and fair in all of our business interactions with customers, patients, members, payers and vendors. The Code details how to report a violation or concern about potential illegal or inappropriate actions. Copies of the Code in different languages can also be found online.

Remember to always ask questions when you are in doubt!