Children's Wisconsin

Reminder: Patient Privacy
Inappropriate Access of Patient Information

The protected health information of our patients, clients and research participants is one of Children's Hospital of Wisconsin's most valued assets. We are entrusted to view, use or forward this information only for appropriate and legitimate purposes. The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations were enacted to hold organizations and individuals accountable for the protection of this information. Generally, if you need the information to do your job, you're probably complying with the rules. Curiosity or "I didn't know" are never acceptable reasons for looking at health information that you shouldn't be accessing or disclosing.

All patients are entitled to privacy and confidentiality of their health information, including VIPs, high profile individuals and family members of Children's employees.

Examples
Following are examples of when accessing and disclosing health information is **NOT** appropriate.

- You decide to look at the scheduling system to confirm that a co-worker is actually attending doctor appointments for his or her children and to determine what illness the children might have.
- Your sister wants to send a card or gift to the child of a friend that she knows who is having surgery. You search for the child's name in the registration database.
- A high profile medical case that is performed at the hospital is being talked about in the news. You are not involved in the patient's care but review the medical record "just to look."
- Your supervisor is going to be on medical leave for a few weeks to care for a family member. You decide to look at the medical record of the supervisor's children to determine one of them has a medical issue that is causing your supervisor's absence.
- Your neighbor tells you another neighbor's child is coming to a clinic that day, and he or she is worried about the reason for the clinic visit. You don't want her to worry, so you determine the reason for the visit.

User id and password
You are solely held accountable for your account access. No one other than you should know your password. Therefore, you shouldn't write your password down or share it with anyone. For instance, allowing a new employee to use your account because he or she hasn't received training and hasn't been assigned a user id and password is not compliant with HIPAA.

Most importantly, once you log-on to the system you never should let anyone else use the same session. Any actions performed will be tracked to your user id, and you will be responsible for any information accessed inappropriately.

Tracking information
The electronic health record system tracks who accesses specific patient electronic records, when those records were accessed and actions taken on those records. The detail of the tracking can be as specific as the user, the workstation, the module and specific activity, the date, the time of day and how long a screen was viewed. The appropriateness of individuals' access and use of health information is assessed according to their job duties.

Accountability process
You will be held accountable and can be terminated for disclosing and/or viewing health information inappropriately. Remember, if you need the information to do your job at Children's, you're probably complying with the rules. If you're looking at health information because you're curious, you're in violation of our policies and the law.