Practical Application Tips for Nursing Students

Usernames & Passwords	1. Never share your NCH username and password! 2. Login to http://employee.nationwidechildrens.org to set your magic questions. If you forget your password, you can self-reset at the same URL! 3. If you suspect someone might be using your login information, immediately report it to an NCH clinical leader.
Accessing PHI	1. To use, share, or access PHI, you have to have a business "need to know." Curiosity or concern over a patient does NOT meet "need to know" requirements! 2. If you are providing care to a patient or conducting a business task for a patient, you have a qualified business need to use, share, or access that patient's PHI.
E-mail	1. Do not use personal e-mail accounts to transmit PHI or other confidential information. 2. Do not text or page PHI.
Portable Media	1. Never copy PHI to personal devices or computers! This includes jump drives, portable hard drives, tablets, phones, etc.
PHI on Paper	1. Do not take PHI off hospital property! This includes patient information recorded on or in: - Notepads - Binders - Patient lists or schedules - Charts - Scrap paper with PHI on it - Print-outs from Epic - Anything else containing PHI
Social Media	1. Once you are on-site at NCH, review our Social Media Policy. 2. Never "friend" a patient! 3. Do not represent NCH on social media. 4. Maintain professional boundaries…avoid interactions that could reflect negatively on NCH. 5. Do not act as a representative of NCH without appropriate approval.
Photos & Videos	1. It is never appropriate to use a personal cell phone to photograph patients or patient information. 2. Photos or videos of patients require authorization from NCH clinical staff. Alert the patient's RN if a photograph or video is needed…they will know the appropriate steps to take.

Completing Assignments/ De-identifying Patient Information	1. Patient information must be completely de-identified prior to using it in any school assignment. 2. All of the following must be stripped: a. Names b. Addresses c. All elements of dates including: i. Birth dates ii. Admission & discharge dates iii. Date of death d. Telephone and fax numbers e. Email addresses f. Social security numbers g. Medical record numbers h. Full face photos or any comparable images i. Health plan beneficiary numbers j. Account numbers k. Certificate/license numbers l. Vehicle identifiers and serial numbers, including license plate numbers m. Device identifiers and serial numbers n. URLs and IP address numbers o. Biometric identifiers, including finger and voice prints p. Any other unique identifying number, characteristic or code
Reporting Privacy Concerns	1. Any known or suspected HIPAA violation is required to be reported! 2. Violations can be reported to your manager, the Privacy Office, or Corporate Compliance.