

Patient Confidentiality Policy for the ICM-III Course Participants

In ICM-III you will be encountering both standardized outpatients and hospitalized patients who will be disclosing confidential personal medical information for your educational benefit. It is imperative, both ethically and legally, for students to safeguard private medical information from inadvertent public disclosure. To insure patient confidentiality, the ICM-III Course Directors have enacted the below policies. Compliance with these policies is mandatory for ICM-III participants, and should be adhered to throughout your professional activities.

1. All patient information revealed in the course of any ICM-III patient encounter is strictly confidential.
2. Students may discuss their ICM-III patient encounters with medical educators and fellow students for the purpose of furthering the educational experience. However, the following restrictions apply:
 - a. Cases may be discussed for educational purposes only.
 - b. Patient identifiers (name, SSN, unique job, etc...) or any aspect of the case that could be used to identify the patient may not be discussed.
 - c. Cases may not be discussed in common areas to include hallways, elevators, dining halls, or other places where any part of the discussion could be overheard by non-authorized personnel. Patient information should never be discussed in a public area (e. g. restaurants, public transportation, etc...)
 - d. Cases should not be shared with family members, acquaintances, or anyone not formally involved in the ICM-III educational experience.
 - e. Cases should not be discussed with classmates that have not yet experienced these cases in the context of ICM-III. This is considered a breach of the honor code.
3. All recorded material is confidential, and must be returned to the Simulation Center after completing the self-evaluation. Students will safeguard the tapes against loss, damage, or theft. Students must report lost or stolen videotapes immediately to the Course Director. Recorded material may not be duplicated or permanently stored on any media.
4. Students should view recorded material in private, and not in the presence of family members, acquaintances, or anyone not involved in the ICM-III educational experience.
5. Written H&Ps are confidential. The following privacy measures apply:
 - a. Written H&Ps will not include any patient identifiers (name, SSN, etc...). Demographic information (age and gender) and relevant social history should be included.
 - b. When no longer required, paper copies of the written H&P will be destroyed or shredded. You may not place a legible copy of any written H&P in the trash.
 - c. Written H&Ps will be removed from the computer drives or other electronic storage media when they are no longer required.
 - d. Written H&P files should never be stored on a common use computer.
 - e. Submitting written H&Ps to your preceptor via email or other electronic means is permitted and encouraged. However, prior to sending an H&P electronically, the H&P must be "de-identified" in accordance with HIPPA standards. De-identification standards are attached.
6. Professionalism, including adherence to the ICM-III confidentiality policy, is a course objective, and failure to achieve any course objective is grounds for referral to the Department of Medicine Education Committee for adjudication of your final grade.

De-Identification Requirements

The following items must be removed from the ICM-III written H&P prior to submitting to your preceptor by electronic mail, fax, or other electronic media:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, and zip code
- All dates (except year) directly related to the individual to include:
 - Date of birth
 - Admission date
 - Discharge date
 - Date of death
 - Age if > 89
- Telephone and fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/License numbers
- Vehicle ID, registration, or license numbers
- Device identifiers and serial numbers
- Web URLs
- IP address
- Biometric identifiers (fingerprint, voice, etc...)
- Full face photographic images and any comparable image
- Any other unique identifying number, characteristic, or code

Note: These “de-identification” requirements for electronic transmission of medical information have been adapted from the HIPAA regulations. Many of the items on this list are not part of the usual ICM-III history and physical, and are not expected in the standard ICM-III H&P. However, the full list is provided for your information.

References

1. Eric Marks, ICM-III Medical Communication Lecture
2. DoD HIPAA Training Website, <https://hipaatraining.tricare.osd.mil>