Confidentiality, Electronic Media and Protected Patient Information Policies and Required Guidelines

HIPAA AND ELECTRONIC MEDICAL RECORD (EMR) ACCESS

- **HIPAA**
  Students must be knowledgeable about and abide by Health Insurance Portability and Accountability Act (HIPAA) policies.

- **Access to EMR**
  Access to health information is highly regulated by laws, including HIPAA, which applies to Protected Health Information (PHI). PHI includes all medical, social, demographic, laboratory, imaging, and other data in the electronic medical records systems at hospitals, ambulatory care centers and other healthcare institutions. These laws carry civil and, for some forms of violation, criminal penalties for individuals who break them, as well as sanctions and penalties for institutions that fail to protect health and personal information.

  The underlying ethical principle of the laws and policies is simple: use of protected information is based on a need to do so, whether the need arises from the care of patients or the business of managing that care. Access to WebCIS/Eclipsys, the NYPH electronic medical record, is not permitted without appropriate HIPAA training beforehand. Students are permitted to access patient electronic medical records and other Protected Health Information for patients they are following, cross covering or have directly encountered with their team as part of their clinical clerkships, selectives and electives. They are permitted continued access after the patient is discharged from the hospital or transferred to another service, or when the student rotates off service, as part of the student's medical education at P&S. Access for any other reason is unprofessional, unethical and illegal. Any attempt to access patient information without the need to know will be dealt with severely, including termination of matriculation at the College of Physicians and Surgeons. If a situation arises about which a student is unsure, he or she is encouraged to discuss it with the supervising attending or with the course director.

- **Access of data for research**
  An important exception to the regulations outlined above is research data. Research data should always be accessed under an approved IRB protocol to which the student needs to be specifically named. These data are usually, although not always, de-identified (coded), depending on the context of the research.

- **WebCIS/Eclipsys and CROWN Passwords**
  Students must not share their WebCIS/Eclipsys or CROWN password with anyone else and must not use another person's password, under any circumstance. Students will be held accountable for any breaches that occur using their password. Some of the most serious problems that have arisen have occurred

because of password sharing. Breaches may under law be reportable to the government and to the patients involved.

When a student is provided with an access code for WebCIS/Eclipsys, they sign a legal document that states they will use this information only to provide patient care and in the context of the need to know. At CUMC there is a specific computer screen which appears when an individual attempts to access information about a patient who has a special relationship to the institution. That screen must be overridden to continue in the quest of information. If an individual overrides that screen without the need to know, they have breached the privilege granted them.

STUDENT ENTRIES INTO THE ELECTRONIC HEALTH RECORD (EHR)

The guidelines below address some common issues that students encounter when given access to computer-based clinical data, but do not cover all possible situations. When in doubt, students should ask the course director how to handle a specific situation.

- **Note writing requirements and use of copy and paste**

  Students are expected to enter notes on the patients they are following in their clinical rotations. NYPH policy states that all student notes must be read, corrected and co-signed by a resident or attending physician within 24 hours.

  Creating an electronic medical record that facilitates excellence in patient care, meets requirements for billing compliance, and constitutes a suitable legal record that requires attention and vigilance. Legal, ethical, and billing compliance principles that apply to electronic documentation are no different from those governing traditional handwritten notes. However, there are two fundamental differences between the paper record and the electronic health record (EHR). First, EHR's have built in "support tools" like Copy Forward that can be simultaneously helpful and dangerous. Second, EHR's have audit logs that track every keystroke.

1. Notes should be concise, accurate, non-redundant, and easy to read.
2. Notes should be completed in a timely manner and emphasize what took place on the day of service.
3. Special emphasis should be placed on the Discussion and Plan portions of the note to clearly communicate the clinical reasoning behind the plan for diagnostic work up, or the pros and cons of particular treatment decisions.
4. "Copy and Paste" and "Copy Forward" should be used with extreme care.
   a. Copying and pasting text without attribution from another provider (most egregiously, another's HPI, but including, for example, a radiology report without attribution) is plagiarism and from a billing perspective, fraud.
   b. It is acceptable in some settings to copy forward lists (e.g. problems, allergies, medications, social history items) as long as they are always *reviewed and updated* and do not clutter the note. Bringing forward previous history critical to longitudinal care is encouraged, so long as it

always *reviewed and updated.* Copy forwarding other elements of history, physical examination or formulations is risky, as errors in editing may jeopardize the credibility of the entire note.

c. Copying and pasting laboratory and radiology reports should be avoided. Important results should be noted, interpreted, and any actions taken should be documented. Wholesale importation of information readily available elsewhere creates clutter, is unnecessary, and may adversely affect physician-to-physician communication.

5. Notes must only be entered in the EHR. Using any non University or Hospital supported system (such as Google docs or gmail) for composing notes or communicating patient information is a violation of University policy and jeopardizes patient privacy.
6. Providers are required to author their own notes. EHR's permit multiple providers to co-author a given note if they are jointly providing a given service, but the attending physician must review, contribute his/her own content, and sign as the ultimate owner of each note for his/her patients. Providers must never share their password and never edit or otherwise change the content of another provider's EHR note if they were not involved in providing that particular service.
7. Once a note is finalized, an addendum can be added to document additional clinical information.
8. All Health Record documentation can be read by others and audited and should be written accordingly.

Following these guidelines will help to ensure safe and effective documentation practices that serve patients well, enable robust communication and care coordination, and protect providers from professional liability.

- **Order Writing Policy**

NYPH policy states that medical students cannot practice medicine and therefore, are not permitted to order medications, and/or any medical treatments or regimes. Orders via the electronic system may not be entered by a medical student using the password of the graduate staff member or attending who is the authorized user. Unauthorized or improper use of the system or the information in it may result in dismissal and civil or criminal penalties. Students must never give verbal orders.

While these policies have been developed specifically in collaboration with NYPH, they pertain to student activities at all other sites.

OTHER ELECTRONIC MEDIA: CONFIDENTIALITY AND SECURITY

Students are responsible for the security of confidential, sensitive and protected patient information (digital and paper-based), and are prohibited from posting images or other patient information on social networking sites or anywhere else on the internet.

- **Social networks**
  Students must be knowledgeable about and abide by the CUMC Guidelines for Social Media.

- **Secure email**
  Students must use only Columbia University email systems for patient and Columbia matters and must not auto-forward Columbia University email to Gmail or other unapproved and unsecure email systems.

- **Devices**
  Students must encrypt portable devices (e.g., laptops and USB drives, etc.) used to store patient or individual research data, and encrypt data files with Protected Health Information (PHI) if stored on a portable device that is not encrypted.

- **Photos**
  Students must not take photos or videos of patients except for purposes of documentation in the medical record, and then, only with prior written consent of the respective institution and when possible, of the patient. Such images may not leave CUMC on a student's electronic device and may not be transmitted in any way other than from one approved email system to another approved email system and only to those caring for the patient.

- **Use of electronic devices in classroom and clinical settings**
  Professional behavior in medical school includes the expectation that students demonstrate their undivided attention when rounding, at the patient bedside, and in didactic sessions. Cell phones, laptops, and other electronic devices can provide a student with access to up to date information related to classroom material and patient care. However, use of these devices must be limited so as to not interfere with lectures, patient care delivery, and team discussions. Students are expected to use judgment when using these devices.

COPYRIGHT & NETWORK USE

- **Copyright**
  Copying, storing, displaying or distributing copyrighted material using University systems or networks without the express permission of the copyright owner, except as otherwise allowed under the copyright law, is prohibited. Under the Federal Digital Millennium Copyright Act of 1998, infringements of copyright by a user can result in termination of the user's access to University systems and networks.

- **Network Use**
  In addition to copyright violations, file sharing programs consume substantial bandwidth drawn on the Columbia University Medical Center network. Since the network's goal is to serve the needs of the hospital, research and teaching, including the NYPH WebCIS (Web-based clinical information system), vital in

the delivery of health care, bandwidth consumption from non-essential sources delays and can compromise patient care, research and teaching. Unhindered network connectivity to conduct everything from scientific data searches to the running of video conferencing is essential. File sharing copyrighted material from unauthorized sources is unethical and against the law, and compromises the security of the source computer and increases the vulnerability of the University network to hackers. Breach of Columbia University policy will result in immediate disconnection of the I.P. of the offending party.

Violations are subject to Dean's Discipline policies.