HIPAA Training for Temporary Employees

The School of Medicine on-line HIPAA training is a valuable educational tool for all employees - both permanent and temporary. Often times it may seem easier to not have a temporary employee complete HIPAA Privacy and Security training but not doing so can lead to a privacy/security incident that could have some pretty serious consequences.

Recently, a temporary employee within the School of Medicine used WebCIS to access the medical record of their immediate supervisor. This security incident was discovered during a routine monthly audit conducted by the hospital.

Upon further investigation, it was determined that the temporary employee had not completed the required HIPAA training modules, General Privacy and General Information Security. UNC School of Medicine requires that all employees, including temporary employees, receive HIPAA Privacy and Security training.

REMEMBER:

Inappropriate access to a patient’s medical record is in violation of UNC HCS policy and is a serious matter subject to disciplinary action.

UNC HCS POLICY

UNC HCS is committed to protecting the privacy of every patient’s medical record and our policy states that physicians, temporary and permanent employees and students should only access medical record information as necessary to perform their job related functions or studies.

The level of auditing of staff and student access into patient records has been increased. Using a combination of automated and manual review, audits are now conducted on a monthly basis.

Things to remember:

- Physicians, employees and students should not discuss medical information except as necessary to perform their job related functions or studies;
- Any access from an employee or student’s login will be attributed to that employee/student, so logging off before walking away from the computer is very important;
- If a friend or family member asks you to look into his/her record, or provide information and feedback that would require access to his/her information, you must have a signed authorization on file in Medical Information Management before using your access to view patient records;

- Patients have the right to “opt out” of patient listings that are typically available at the information desk. If the patient “opts out,” we are not allowed to even acknowledge that the patient is here;

- Individuals using WebCIS or other operational/clinical systems to look up a patient room number may be logged as violating a patient’s privacy if the patient has opted out of patient listings. An assistant looking up information for a physician, administrator, or supervisor may also violate the patient’s privacy if the reason for the access is not related to treatment, payment, or health operations;

- Celebrities and publicly known individuals have the same rights to privacy as anyone else, and the higher exposure that follows these patients complicates privacy violations. Physicians, employees or students should not surf for patients looking to see if a patient will be assigned to their service, unit, or otherwise might be interesting;

- Remember, curiosity is never an acceptable reason to access a patient’s medical record;

- Unless the patient has specifically asked you to notify their church, friends or family members, doing so is in violation of the patient’s privacy rights.

- Access of information on a party to a divorce, separation, break-up, or custody dispute is an indication of intent to use information for personal advantage, and will be considered in the application of sanctions.

- Physicians, employees and students have a responsibility to protect patient information, and should report violations to the Privacy Office, Compliance, or to Medical Information Management.

- Authorization Form – MIM #710-S Release of Medical Information should be completed and submitted to MIM prior to accessing medical records.

To review the UNC School of Medicine on-line HIPAA Privacy and Security training click on the link: [http://www.med.unc.edu/security/hipaa](http://www.med.unc.edu/security/hipaa)

*Created by Jane Teeter*