THE UNIVERSITY OF NORTH CAROLINA
AT CHAPEL HILL

PROTECTED HEALTH INFORMATION (PHI) CONFIDENTIALITY STATEMENT

As a user of information at UNC-Chapel Hill, you may develop, use, or maintain patient information for health care, quality improvement, peer review, education, billing, reimbursement, administration, research or for other approved purposes. This information, from any source and in any form, including, but not limited to, paper record, oral communication, audio recording, and electronic display, is considered confidential. Access to confidential information is permitted only on a need-to-know basis and limited to the minimum amount of confidential information necessary to accomplish the intended purpose of the use, disclosure or request.

It is the policy of UNC-Chapel Hill that users (i.e., employees, medical staff, students, volunteers, vendors and other outside affiliates) shall respect and preserve the privacy, confidentiality and security of confidential information. **Violations of this statement include, but are not limited to:**

- **accessing confidential information that is not within the scope of your duties;**
- **misusing, disclosing without proper authorization, or altering confidential information;**
- **disclosing to another person your sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas;**
- **using another person's sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas;**
- **intentional or negligent mishandling or destruction of confidential information;**
- **leaving a secured application unattended while signed on; or**
- **attempting to access a secured application or restricted area without proper authorization or for purposes other than official UNC-Chapel Hill business.**

Violation of this PHI Confidentiality Statement may result in disciplinary action, up to and including termination of employment or student status, and/or loss of University System privileges or contractual or affiliation rights in accordance with applicable University procedures. Unauthorized use or release of confidential information may also subject the individual to personal, civil, and/or criminal liability and legal penalties.

EXAMPLES OF BREACHES OF CONFIDENTIALITY

Accessing confidential information that is not within the scope of your duties: Unauthorized reading of patient account information; Unauthorized reading of a patient's chart; Unauthorized access of personnel file information; Accessing information that you do not "need-to-know" for the proper execution of your duties.	**Misusing, disclosing without proper authorization, or altering confidential information:** Making unauthorized marks on a patient's chart; Making unauthorized changes to a personnel file; Sharing or reproducing information in a patient chart or a personnel file with unauthorized personnel; Discussing confidential information in a public area such as a waiting room or elevator.
Disclosing to another person your sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas: Telling a co-worker your password so that he or she can log in to your work or access your work area; Telling an unauthorized person the access codes for personnel files, patient accounts, or restricted areas.	**Using another person's sign-on code and/or password for accessing electronic confidential information or for physical access to restricted areas:** Using a co-worker's password to log in to the University computer system or access their work area; Unauthorized use of a login code for access to personnel files, patient accounts, or restricted areas.
Intentional or negligent mishandling or destruction of confidential information: Leaving confidential information in areas outside of your work area, such as the cafeteria or your home. Disposing of confidential information in a non-approved container, such as a trash can.	**Leaving a secured application unattended while signed on:** Being away from your desk while you are logged into an application. Allowing a co-worker to use your secured application for which he or she does not have access after you have logged in.
Attempting to access a secured application or restricted area without proper authorization or for purposes other than official University business: Trying passwords and login codes to gain access to an unauthorized area of the computer system or restricted area; Using a co-worker's application for which you do not have access after he or she is logged in.	**The examples above are only a few types of mishandling of confidential information. If you have any questions about the handling, use or disclosure of confidential information please contact your supervisor, manager, or director.**