The University of North Carolina-Chapel Hill School of Nursing

UNIVERSAL CONFIDENTIALITY STATEMENT

As a student or faculty member participating in an academic course, laboratory session or assigned to a clinical agency via contractual agreement or Memorandum of Understanding, you are allowed access to the personal health information and/or medical records of clients, employees, research subjects, and operational business information (specific to the agency and/or its affiliated third parties, and licensed products or processes). Information specific to student colleagues, faculty, patients/clients, employees or subjects from any source and in any form, including, but not limited to, paper records, oral communication, clinical examination, pictures, audio/ video recordings, electronic display, course materials and research data files is strictly 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 the UNC-Chapel Hill School of Nursing that students, faculty, and staff of the School shall respect and preserve privacy, confidentiality and security of confidential information, regardless of the academic course, laboratory or clinical agency to which the student or faculty is assigned. **Violations of this policy include, but are not limited to:**

- **accessing confidential information that is not within the scope of your assignment;**
- **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;**
- **use of any e-mail account other than a UNC Exchange e-mail account for conveying information related to an academic course, clinical assignment, research endeavor or other School of Nursing activity. Neither Microsoft Live@unc.edu (also known as HeelMail) nor any external e-mail services such as Gmail, AOL, Yahoo, etc. are to be used.**
- **leaving a secured application unattended while signed on;**
- **attempting to access a secured application or restricted area without proper authorization or for purposes other than official business;**
- **failing to take proper precautions for preventing unintentional disclosure of confidential information;**
- **failing to properly secure research data files;**
- **posting/discussing confidential information via text messages, electronic mail, and/or any electronic social network sites (e.g., Facebook, Twitter, etc.);**
- **using personal cell phone or similar device to take unauthorized pictures or audio/video recordings involving confidential information, and transmitting them electronically; OR**
- **distributing, disseminating, modifying or otherwise copying digital course materials including those found on Blackboard or other course websites;**

Violation of this statement may constitute grounds for corrective action up to and including loss of agency privileges, academic or employment suspension, or termination from the School in accordance with applicable agency, School or University procedures. Violation of this policy by any member of the School's student body, faculty or staff may constitute grounds for termination of the contractual relationship or other terms of affiliation between the School and the agency. Unauthorized release of confidential information may also subject the violator to personal, civil, and/or criminal liability and legal penalties. Knowledge of any student/faculty member in violation of these policies should be reported to School of Nursing's Associate Dean for Academic Affairs. Student violators will be referred to the University's Honor Court for resolution; faculty and staff violators will be addressed by School administration.

I have read, understand and agree to comply with the terms stated herein. Further, I will read and comply with all University, School of Nursing and clinical agency policies and standards relative to confidentiality and information security. A copy of the School's Information Security Policy is attached.

Please check one: □ BSN Student □ MSN student □ Post-MSN student □ PhD Student

________________________________ __________________________
Printed/Typed Name Personal Identification Number

________________________________ __________________________
Signature Date

Revised: 02/03; 02/04; 03/06; 10/07; 1/09; 08/10; 10/11 (draft)

The University of North Carolina-Chapel Hill School of Nursing

INFORMATION SECURITY POLICY

Policy

Information, as hereinafter defined, in all its forms and throughout its life cycle will be protected in a manner consistent with its sensitivity and value to any academic course or clinical agency to which a student, staff or faculty member is assigned via contractual agreement or Memorandum of Understanding between the School of Nursing and the agency. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit information.

This policy applies to all situations in which sensitive information is accessible from any source and in any form, to include clinical information generated in the context of patient care, course requirements or clinical research. This information may be available through, but not limited to, paper records, oral communication, health/laboratory/evaluative/diagnostic/examination findings, pictures, audio/ video recordings, electronic display, course materials , research data files, personnel records and operational information. Such client/employee/subject-related data may be available electronically, digitally, or in written form in standard medical records, patient charts, course materials, employee files and/or business documents. It may be available for individual or groups of clients/employees/subjects. Such information may reside in large central computer databases, such as those maintained by large hospitals and academic health centers where it can be made available electronically to peripheral workstations, such as clinical workstations or peripheral clinical or personnel databases maintained by individual agency personnel. It may also reside in databases that are separate from the centrally maintained databases, such as the academic, clinical, operational, personnel or research databases that have been developed by certain agency personnel members or stored digitally on academic websites.

Scope

The scope of information security is protection of information that is written, spoken, recorded electronically, transmitted digitally or printed, from accidental or intentional misuse, modification, mishandling, destruction or disclosure. Information will be protected throughout its life cycle (origination, entry, processing, distribution, storage, and disposal).

EXAMPLES OF BREACHES OF CONFIDENTIALITY

Accessing information that is not within the scope of your job/role as student, staff or faculty member: • Unauthorized reading of client/employee/subject account information; • Unauthorized reading of a client's/subject's chart; • Unauthorized access of personnel file or business/ operational information; • Accessing information that you do not "need-to-know" for proper execution of your job functions.	**Misusing, disclosing without proper authorization, or altering patient or personnel information:** • Making unauthorized marks on a medical record; • Making unauthorized changes to a personnel file or research data files; • Sharing or reproducing information in a client's/subject's chart or 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; • Telling an unauthorized person the access codes for personnel files or patient accounts.	**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 hospital's computer system; • Unauthorized use of a login code for access to personnel files or client/subject information, or restricted areas.
Intentional or negligent mishandling or destruction of confidential information: ▪ Leaving confidential information in areas outside your work area, e.g. 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 the desk area while logged into an application; • Allowing another person 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 business: • Trying passwords and login codes to again 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.	**Unintentional disclosure of patient information:** • Failure to take necessary precautions to properly prevent unauthorized viewing of displayed confidential information in public areas; • Discussing confidential patient information in public areas; • Inappropriately removing documents containing confidential information from clinical areas. • Using an email account *other than* a UNC exchange email account for conveying course/clinical/research/other School related business
Intentional dissemination of confidential information • Distributing sensitive information via text, email, Facebook, etc. • Electronic or digital transmission of unauthorized pictures or audio/video recordings	**Intentional and unauthorized distribution, dissemination, modification or copying digital course materials**

The examples above are only a few types of mishandling of confidential information. If you have any questions about the proper handling, use, or disclosure of confidential information, please contact your supervisor or supervising faculty member immediately.

Revised: 02/03; 02/04; 03/06; 10/07; 1/09; 08/10; 10/11 (draft)