Confidentiality Statement

It is the policy of the UNC Health Care System and its affiliates (individually and collectively called "UNC HC" herein) that users (i.e., employees, medical staff, students, volunteers, contractors, vendors, outside affiliates, and any others who are permitted access to UNC HC systems and/or UNC HC information) shall respect and preserve the privacy, confidentiality and security of confidential information ("CI") which shall include: (1) individually identifiable patient information in any format including but not limited to paper and electronic medical and billing records, (2) personnel information (e.g., disciplinary or other information about employees, volunteers, students, contractors, or medical staff), (3) confidential business information of UNC HC and/or third parties, including third-party software and licensed products or processes, or (4) other nonpublic information including information on operations, quality improvement, peer review, education, billing, reimbursement, administration, or research (such as utilization reports, survey results, and related presentations). CI may be created internally or received from other institutions and may be in any format including paper, verbal/oral communication, audio recordings or electronic format. **I understand and agree that I will only access, maintain, use or disclose CI for legitimate job-related, need-to-know purposes.**

I further agree that:

1. I will protect the privacy, confidentiality and security of UNC HC patient information at all times in accordance with federal and state regulations and applicable UNC HC policies and procedures.
2. I will complete all required information privacy and security training required by UNC HC policies and procedures.
3. I will not maintain CI on any unencrypted portable computing device (laptop, smartphone, tablet, etc.) and I will not electronically transmit CI in an unsecure manner.
4. I will not disclose my user name and/or password for any UNC HC system, application or device to which I have access; I will not use another person's user name and password to access CI on any UNC HC electronic system; and I will not leave any system, application or computer containing CI unattended while I am signed on.
5. I will not attempt to access any CI in electronic format on any UNC HC system, application or device or access a restricted physical area containing CI without proper authorization or for purposes other than official UNC HC business.
6. I will only alter or destroy CI in accordance with applicable UNC HC policies and procedures.
7. I will immediately report to my supervisor (or the appropriate UNC HC office) any known or suspected incident involving the unauthorized access, use or disclosure of CI and I will fully cooperate in any resulting investigation and make myself available for all related interviews and provide all relevant information requested during such investigation.
8. I will safeguard from loss, theft, or unauthorized use/access UNC HC owned equipment/property on which CI is stored or through which CI may be accessed. I will immediately notify the UNC HC Information Security Department if any portable computing device I use to store or access CI is lost or stolen.
9. I will not store or transmit CI on my personal equipment/property (such as personally owned computing devices) unless permitted by and in accordance with applicable UNC HC policy or procedure.
10. I will abide by UNC HC social media policies at all times and I will never post patient identifiable information on social media in violation of UNC HC policy.
11. I will not take photographs, make videos, or make other recordings of patients, staff, or visitors except in accordance with applicable UNC HC policies and procedures.
12. I understand that my access to CI on UNC HC electronic systems and my UNC HC email account may be audited.
13. I will not access or obtain my own, a friend's, or a family member's patient information maintained by UNC HC without appropriate written authorization and under applicable policies and procedures.

I agree that I have read, understand and will comply with the terms of this Confidentiality Statement. I understand that my failure to comply with this Confidentiality Statement may result in termination of access to UNC HC electronic health records , personal civil or criminal legal penalties, disciplinary action (up to and including termination of employment or student status), or loss of UNC HC privileges or contractual or affiliation rights. AFTER MY EMPLOYMENT OR WORK AT UNC HC ENDS, I WILL NOT TAKE ANY CONFIDENTIAL INFORMATION WITH ME AND I WILL NOT FURTHER USE OR DISCLOSE ANY CONFIDENTIAL INFORMATION.

Name: _____ Employee ID or email address: _____
(please print)

Entity (e.g., UNC Hospitals): _____

Affiliation:
☐Employee ☐Temporary Employee ☐Contractor ☐Medical Staff ☐Resident ☐Referring Physician ☐Student ☐Other Providers
☐ Volunteer ☐Vendor (specify): _____ ☐Other (specify):_____

Signature:_____ Date: _____

Last revised February 27, 2018

Examples of Breaches of Confidentiality

Accessing confidential information that is not within the scope of your duties: Unauthorized access or reading of patient medical or account information; Unauthorized access of personnel file information; Accessing information for which you do not have a legitimate job-related "need-to- know" purpose for the proper execution of your duties.	**Misusing, disclosing without proper authorization, or altering confidential information:** Making unauthorized entries into or marks on a patient's chart or electronic medical record; 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 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 into your work or access your work area; Telling an unauthorized person the access codes for personnel files, patient accounts, or restricted areas; Posting passwords and sign-on codes in a location where they may be viewed by others.	**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 UNC Health Care 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; Failure to promptly report the loss or theft of UNC Health Care owned equipment/property assigned to you or the misuse of this equipment/property; Failure to report the loss or theft of personally owned equipment containing UNC Health Care confidential information.	**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; Taking or allowing photographs to be taken of patients or patient PHI without obtaining the required authorization; Posting photos or confidential information on social medial or public access point.
Attempting to access a secured application or restricted area without proper authorization or for purposes other than official UNC Health Care 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.	**These examples are only a few examples 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.**