Confidentiality Statement

As a user of information at the Washington Institute for Coagulation d/b/a Washington Center for Bleeding Disorders, you may develop, use, or maintain (1) patient information (for health care, quality improvement, performance review, education, billing, administrative responsibilities, research, or for other business purposes), (2) personnel information (for employment, payroll, or other business purposes), or (3) confidential business information of WACBD and/or third parties, including third-party software and other licensed products or processes. This information from any source and in any form, including, but not limited to, paper record, oral communication, audio recording, electronic display, and electronic communication 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.

Users (i.e., employees, medical staff, students, board members, and outside affiliates) shall respect and preserve the privacy, confidentiality and security of confidential information. Users also have a responsibility to report any misuse, abuse, or breach of PHI and other confidential information. **Violations of this statement include, but are not limited to:**

- Accessing 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-in credentials and/or password for accessing electronic or confidential information or for physical access to restricted areas;
- Using another person's sign-in credentials 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 in; or
- Attempting to access a secured application or restricted area without proper authorization or for purposes other then official WIC business.

Violation of this statement may constitute grounds for corrective action up to and including termination of employment or student status, loss of WACBD privileges or contractual or affiliation rights in accordance with applicable WACBD procedures. Unauthorized use or release of confidential information may also subject the violator to personal, civil, and/or criminal liability and legal penalties.

By signing below, I certify have been informed on and understand WACBD policies including related federal and state laws and regulations related to the Health Insurance Portability and Accountability Act (HIPAA) and privacy and security practices. I understand that I must protect the privacy and security of all patient protected health information (PHI) and employee information created, obtained and held by WACBD.

Name: _____
(please print)

Employee ID or last 4 Digits of SSN: _____

Affiliation:

[ ] Employee [ ] Contract Employee
[ ] Fellow [ ] Resident
[ ] Referring Physician [ ] Student
[ ] Other Providers [ ] Board Member
[ ] Vendor (specify): _____
[ ] Other :_____

Signature/Date: _____ / _____
(please sign) Date

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 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-in code and/or password for accessing electronic confidential information or for physical access to restricted areas:** Using a co-worker's password to sign-in to NextGen or CPR+, WIC's Electronic Medical Record Softwares. Unauthorized use of a sign-in 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 your home or other location outside of your work area. Disposing of confidential information in a non-approved container, such as a trash can.	**Leaving a secured application unattended while signed in:** Being away from your desk while you are logged into an application. Allowing a co-worker to use your secured application for which they do not have access after you have signed-in.
Attempting to access a secured application or restricted area without proper authorization or for purposes other than official WIC business: Trying passwords and sign-in 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 they have signed-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 a director.**