

CONFIDENTIALITY/SECURITY OF INFORMATION & COMPUTER ACCESS CODE AGREEMENT

During your clinical experience at Northside Hospital (“NSH”), it may be necessary to have access to NSH patient, medical, financial, employee, organizational, and other types of information while on campus. You have a duty, and must agree to protect the confidentiality and security of all such information. You should treat any and all information to which you are exposed during the course of your clinical experience at NSH as highly confidential and will not disclose such information to anyone who does not need that information to perform his/her professional duties. This applies to all sources of information and methods of communication including, but not limited to, computer systems, personal digital assistants (PDAs), paper documents, faxes, email, telephone, and direct verbal communication.

Each student/clinical instructor must complete the following and the clinical instructor must sign the Confidentiality Agreement of Information and Computer Access Code Agreement.

Dept. Name or Name of Agency: Write the name of your school

Employee/Agent’s Signature: All students must sign

Employee/Agent’s Position: Write specialty type (RN, LPN, etc.)

Manager/NSH Designee’s Signature: The clinical instructor or school representative must sign as the NSH designee.

Page two of the Confidentiality Agreement should be uploaded in CredentialLink as part of the initial credentialing process.



NORTHSIDE HOSPITAL

Confidentiality/Security of Information and Computer Access Code Agreement

As an employee or agent of Northside Hospital (“NSH”), it may be necessary to have access to NSH patient, medical, financial, employee, organizational, and other types of information to perform my job responsibilities. I recognize that as an employee or agent, I have a duty, and agree, to protect the confidentiality and security of all such information. I will treat any and all information I am exposed to during the course of my employment or affiliation with NSH as highly confidential and will not disclose such information to anyone who does not need that information to perform his/her professional duties. This applies to all sources of information and methods of communication including, but not limited to, computer systems, personal digital assistants (PDAs), paper documents, faxes, email, telephone, and direct verbal communication.

Furthermore, I acknowledge the following:

1. I will not use or disclose protected health information (“PHI”), as defined by the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (“HIPAA”), in a manner that would violate the privacy and security standards promulgated by HIPAA contained at 45 C.F.R. Part 164. I agree to implement necessary safeguards and prevent the unauthorized use or disclosure of PHI that I am exposed to during the course of my employment with NSH.
2. I will not access PHI unless I have a need to know this information to perform my job or duties. I further acknowledge that I will not access PHI associated with my spouse, children, other relatives, friends, staff or colleagues except to the extent necessary to perform my job or duties.
3. I will not disclose PHI to any person or entity, other than as necessary to perform my job or duties and as permitted under HIPAA.
4. Upon cessation of my employment or affiliation with NSH, I agree to continue to maintain the confidentiality of any information I learned while employed by or affiliated with NSH and agree to turn over any keys, access cards, or other devices that would provide access to NSH information and computer systems.
5. I understand that only those individuals who have signed a “*Confidentiality/Security of Information and Computer Access Code Agreement*” will be given access to NSH information systems. I understand that all employees and agents are required to sign this Agreement, and I further understand that I will not be provided access to NSH’s information systems unless I have signed this Agreement acknowledging my agreement to be bound by its terms.
6. The combination of my username and password to all NSH information systems is the legal equivalent of my signature. I will not disclose my username or password to anyone under any circumstances. If I suspect or have any reason to believe that my username or password are or may be known by others, I will notify my supervisor or the Information Systems Department immediately to have the information changed.
7. I will not write down or otherwise document my username where it may potentially be viewed by another individual. I will not write down my password anywhere but rather will commit it to memory.
8. I will not attempt to learn another user’s username or password nor will I use any username or password other than my own.
9. I understand that access to the NSH information systems is a requirement for many positions within the organization and computer system access should be used with the utmost discretion. At no time am I authorized to utilize any NSH system for any reason other than its intended use to perform my professional duties nor may I use it for my own or other’s personal or professional gain.



NORTHSIDE HOSPITAL

Confidentiality/Security of Information and Computer Access Code Agreement

- 10. Once I have signed onto any NSH information system, I will not allow anyone else to use the information system for any reason, including to access patient, medical, financial, employee, organizational, or any other type of information.
- 11. I will ensure that my use of NSH computers, email, computer accounts, and networks as well as information accessed, stored, or used on any of these systems is restricted to authorized duties or activities.
- 12. I will not download, install, or run unlicensed or unauthorized software on any NSH system.
- 13. When I leave the immediate physical vicinity of a PC, laptop, or other workstation upon which I am signed into any NSH system (whether on any NSH campus or a remote site), I will ensure that I properly log out of the system.
- 14. If I have remote access to any of NSH's information systems, I will ensure appropriate security measures are implemented and maintained on the remote PC or device. Furthermore, I will ensure no PHI is downloaded or otherwise stored on the remote PC or device unless the device is approved to store PHI and utilizes NSH approved encryption technologies to secure such data. I will take all reasonable and practical measures to minimize the risk of unauthorized access to NSH's information systems. I understand that all terms and conditions of this agreement apply equally whether the systems are being accessed on any of NSH's campuses or from any remote site.

I have read and fully understand the above and agree to be bound by each and every term and condition of this agreement as well as Administrative Policies and Procedures "*Privacy/Confidentiality of Patient Information*" and "*Information Security Policy and Procedure*". If I violate any of these agreements, I understand that I may be subject to disciplinary actions pursuant to "*HR 611 Progressive Discipline Policy*," up to and including termination of employment.

Printed Name: _____ Dept. #: _____

Dept. Name or Name of Agency: _____

Employee/Agent's Signature: _____ Date: _____

Employee/Agent's Position: _____ Date: _____

Manager / NSH Designee's Signature: _____ Date: _____