DUKE CONFIDENTIALITY AGREEMENT

I agree to protect the confidentiality, privacy and security of patient, student, personnel, business, and other confidential or proprietary information of Duke University, Duke University Health System and the Private Diagnostic Clinic (collectively, "Duke") from any source and in any form (talking, paper, electronic). I understand that the kinds of confidential or proprietary information that I may see or hear on my job and must protect include the following, among others:

PATIENTS AND/OR FAMILY MEMBERS (such as patient records, conversations and billing information)

EMPLOYEES, VOLUNTEERS, STUDENTS, CONTRACTORS, PARTNERS (such as salaries, employment records, disciplinary actions)

BUSINESS INFORMATION (such as financial records, research or clinical trial data, reports, memos, contracts, computer programs, technology)

THIRD PARTIES (such as vendor contracts, computer programs, technology)

OPERATIONS IMPROVEMENT, QUALITY ASSURANCE, MEDICAL OR PEER REVIEW (such as reports, presentations, survey results**)**

I AGREE THAT:

1. I WILL protect Duke confidential or proprietary information in any form. I WILL follow Duke policies, procedures and other requirements on privacy and security.
2. I will keep current on all required training on the privacy and security of confidential or proprietary information.
3. I WILL ONLY access information that I need for my job or service at Duke.
4. I WILL NOT access, show, tell, use, release, e-mail, copy, give, sell, review, change or dispose of confidential or proprietary information unless it is part of my job or to provide service at Duke. If it is part of my job or to provide service to do any of these tasks, I will follow the correct procedures (such as shredding confidential papers before throwing them away).
5. When my work or service at Duke ends, I will not disclose any confidential or proprietary information and I will not take any of this information with me if I leave or am terminated.
6. If I must take confidential or proprietary information off Duke property, I will do so only with my supervisor's permission. I will protect the privacy and security of the information in accordance with Duke policies and procedures and I will return it to Duke.
7. If I have access to Duke computer system(s), I WILL follow their Secure System Usage Memos which are available from the Systems' Information Security Administrator(s).
8. I WILL NOT share my USER ID and password with anyone.
9. I WILL KEEP my computer password secret and I will not share it with anyone.
10. I WILL create a strong password* and change it **at least** every 180 days. I will change my password at once if I think someone knows or used my password. I will ask my supervisor if I do not know how to change my password.
11. I WILL tell my supervisor and OIT or DHTS if I think someone knows or may use my password or if I am aware of any possible breaches of confidentiality at Duke.
12. I WILL NOT use anyone else's USER ID and password to access any Duke System(s).
13. I WILL log out or secure my workstation when I leave my work area.
14. I WILL ONLY access confidential or proprietary information at remote locations with consent from my supervisor.
15. If I am allowed to remotely access confidential or proprietary information, I AM RESPONSIBLE for ensuring the privacy and security of the information at ANY location (e.g., home, office, etc.).
16. I WILL NOT store confidential or proprietary information on non-Duke systems.
17. I UNDERSTAND that my access to confidential or proprietary information and my Duke e-mail account may be audited.
18. If I receive personal information through Duke e-mail or other Duke systems, I AGREE that authorized Duke personnel may examine it, and I do not expect it to be protected by Duke.
19. I UNDERSTAND that Duke may take away or limit my access at any time.

I understand that my failure to comply with this agreement may result in the termination of my relationship with Duke and/or civil or criminal legal penalties. By signing this, I agree that I have read, understand and will comply with this agreement:

Signature:_____ **Date**:_____

Print Full Name:_____ **Dept.** _____

Examples of Breaches of Confidentiality
(What you should NOT do)

These are examples only. They do not include all possible breaches of confidentiality covered by the Duke Breach of Confidentiality policy and this Confidentiality Agreement.

Accessing information that you do not need to know to do your job:

- Unauthorized reading of patient account information.
- Unauthorized reading of a patient's chart.
- Accessing information on family, friends or co-workers.

Sharing your sign-on code and password:

- Telling someone your password so that he or she can log in to your work.
- Giving someone the access codes for employee files or patient accounts.

Sharing, copying or changing information without proper authorization:

- Making unauthorized marks on a patient's chart.
- Making unauthorized changes to an employee file.
- Discussing confidential information in a public area such as a waiting room, elevator, or cafeteria.

Leaving a **secured application unattended while signed on:

- Being away from your computer while you are logged into an application.
- Allowing someone to access confidential information using your USER ID and password.

DEFINITIONS

****Secured Application** = any computer program that allows access to confidential information. A secured application usually requires a user name and password to login.

***Strong Computer Passwords**

- Be at least six characters.
- Contain at least two letters and one number.
- Have at least one Capital letter and one lower case letter.
- Change at least every 180 days or if it is believed or known to have been compromised.
- Not a word in the dictionary
- Not re-used for at least three years.