DUKE CONFIDENTIALITY AGREEMENT

I agree to protect the confidentiality, privacy and security of patient, student, staff, business and other confidential, sensitive electronic or proprietary information (collectively, "Confidential Information") of Duke University, Duke University Health System, Duke University Affiliated Physicians, Duke Connected Care and the Private Diagnostic Clinic (collectively, "Duke") from any source and in any form (spoken, paper, electronic). I understand that I have an obligation to protect the Confidential Information that I may create, access, use or disclose as part of my job including the following, among others:

- **PATIENTS AND/OR FAMILY MEMBERS** (such as patient records, conversations and billing information)
- **MEDICAL STAFF, EMPLOYEES, VOLUNTEERS, STUDENTS, or CONTRACTORS** (such as social security numbers, salaries, clinical information, billing information, employment records, disciplinary actions)
- **BUSINESS INFORMATION** (such as financial records, research or clinical trial data, reports, contracts, computer programs, technology)
- **THIRD PARTIES** (such as vendor contracts, computer programs, technology)
- **OPERATIONS, PERFORMANCE IMPROVEMENT, QUALITY ASSURANCE, MEDICAL OR PEER REVIEW** (such as utilization, data reports, quality improvement, presentations, survey results)

I AGREE THAT:

1. I WILL protect Duke Confidential Information in any form. I WILL follow federal and state statues and regulation and Duke Policies, procedures and other privacy and security requirements ("Duke Policies").
2. I WILL NOT post, discuss, or otherwise share any Confidential Information, including patient pictures or videos, financial or personnel information on any social media sites such as Facebook or Twitter. I WILL NOT post Confidential Information including patient information or pictures on Duke-sponsored social media sites without the appropriate patient authorization in accordance with management approval and Duke Policies and procedures.
3. I WILL NOT take any pictures of patients for personal use with devices or other methods.
4. I WILL complete all required privacy and security training.
5. I WILL ONLY access information that I need to perform my job responsibilities or services at Duke.
6. I WILL NOT access, show, tell, use, release, e-mail, copy, give, sell, review, change or dispose of Confidential Information unless it is part of my job responsibility or to provide service at Duke. I WILL follow Duke Policies (such as shredding confidential papers using confidential Shred-it™ lock bins or deleting electronic files from devices) and only access/use the minimum necessary of the information to complete the required task.
7. When my work or service at Duke ends, I WILL NOT disclose any Confidential Information, and I WILL NOT take any Confidential Information with me if I leave or am terminated.
8. If I must take Confidential Information off Duke property, I WILL do so only with my supervisor's permission and/or in accordance with Duke policies and procedures. I WILL protect the privacy and security of the Confidential Information in accordance with Duke Policies and I WILL return it to Duke.
9. If I have access to Duke computer system(s), I WILL follow the Secure System Usage Memos*.
10. I WILL NOT use another's User ID (Net ID) or password to access any Duke system, and I WILL NOT share my User ID (Net ID) password or other computer password with anyone.
11. I WILL create a strong password** and change it in accordance with Duke Policies. I WILL notify DHTS Security Office and 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.
12. I WILL tell my supervisor and OIT or DHTS Security Officer if I think someone knows or may use my password or if I am aware of any possible breaches of my user name or password. I WILL report suspected breaches of confidentiality to my supervisor or the Compliance Office.
13. I WILL log out or secure my workstation when I leave the computer unattended.
14. I WILL ONLY access Confidential Information at remote locations in accordance with Duke Policies.
15. If I am allowed to remotely access Confidential Information, I AM RESPONSIBLE for ensuring the privacy and security of the information at ANY location (e.g., home, office, etc.).
16. With the exception of accessing Duke email on a personal smartphone (e.g., iPhone or Android device) or tablet (e.g., iPad), I WILL NOT store Confidential Information on non-Duke systems including on personal computers/devices. I WILL immediately report any lost or stolen device, personal or otherwise, that was used to access Duke resources.
17. **I WILL NOT maintain or send Confidential Information to any unencrypted mobile or portable storage device in accordance with Duke Policies.**
18. I UNDERSTAND that my access to Confidential Information and my Duke e-mail account may be audited.
19. 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.
20. I UNDERSTAND that Duke may remove or limit my access to Duke's computer system(s) 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._____

Rev. 08/2015

Examples of Breach 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 Protected Health Information/Patient Privacy policy and this Confidentiality Agreement.

Accessing information that you do not need to know to perform Your job responsibility or services:
• Unauthorized reading of patient account information.
• Unauthorized reading of a patient's chart.
• Accessing information on adult children, friends or co-workers.

Sharing your User ID and password:
• Telling someone your password so that he or she can log into Duke's computer system(s) to do their work or yours.
• Giving someone the access codes for employee files or patient accounts.
• Emailing Confidential Information outside of Duke by unsecure methods (not encrypted).

Sharing, copying or changing information without proper authorization:
• Making unauthorized changes to an employee file.
• Discussing Confidential Information in a public area such as a waiting room, elevator or cafeteria.
• Posting a picture of a patient on a social media site.
• Commenting on a patient on a social media site.

Leaving a secured application* unattended while signed on:**
• Being away from your computer while you are logged into patient billing information.
• Allowing someone to access Confidential Information using your User ID (NET ID) and password.

DEFINITIONS

*** Secure System Usage Memo** – Memo published annually by Duke Medicine's Information Security Office to provide an overview of the information security policies, standards, and procedures that apply to all Duke Medicine faculty, staff, students, and affiliates. Memo can be located at: https://security.duke.edu/policies/duke-medicine-secure-systems-usage-memo.

**** Strong Computer Passwords are defined in the DHE Information Security Standard: Passwords and must be in accordance with Duke IT security policies.**

*** **Secured Application** – any computer program that allows access to Confidential Information. A secured application usually requires a user name and password to log in.