Confidentiality Agreement

I agree to protect the confidentiality, privacy and security of patient, student, staff, business and other confidential, sensitive or proprietary information of Affinity Health Alliance and its affiliated entities (collectively, AHA) in any form (spoken, paper, electronic) (collectively, "Confidential Information"). 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 but not limited to the following:

- **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)

"Confidential Information" does not include any information or knowledge which: (i) is in the public domain through no fault of any AHA employee; or (ii) is disclosed to an AHA employee lawfully by a third party who is not under any obligation of confidentiality. Policy AG-225 contains further description of what constitutes Confidential Information.

I AGREE THAT:

1. I WILL maintain the confidentiality of AHA Confidential Information during my employment with AHA and after my employment ends for any reason.
2. I WILL NOT access, show, tell, use, release, e-mail, copy, give, sell, review, change or dispose of Confidential Information except as necessary to perform my job responsibilities or services at AHA. I WILL ONLY access/use/disclose the minimum necessary information that I need to perform my job responsibilities or services at AHA.
3. I WILL NOT post, discuss, or otherwise share any Confidential Information, including patient pictures or videos, financial or personnel information in public, including on any social media site such as Facebook or Twitter. I WILL NOT post Confidential Information, including patient information or pictures, on AHA-sponsored social media sites without the appropriate patient authorization and approval of the Director of Marketing and Public Relations.
4. I WILL NOT remove Confidential Information from AHA property without my supervisor/manager's permission. I WILL maintain the confidentiality of the Confidential Information I am permitted to remove and return it to AHA as promptly as possible.
5. I WILL take precautions when disposing of Confidential Information (e.g., shredding confidential papers using confidential shred containers/lock bins or deleting electronic files from devices).
6. If I am given access to AHA computer system(s), I will follow AHA policies regarding secure system usage, including the Information Security/HIPAA policies available on the employee Intranet. I UNDERSTAND those policies require that I, among other things:
   - DO NOT share my user ID or password with anyone else, or use anyone else's user ID or password to access any AHA computer system.
   - DO create a strong password and change it periodically. I WILL ask my supervisor if I do not know how to change my password.
   - DO log out or secure my workstation when I leave my computer unattended.
   - DO notify the Privacy Officer if I believe someone else knows or used my password.
   - DO notify the Compliance Officer if I am aware of other possible breaches of confidentiality.
7. With the exception of accessing Union email on a personal smartphone (e.g., iPhone or Android device), tablet (e.g., iPad), or similar device, I WILL NOT store Confidential Information on any unencrypted mobile or portable storage device, such as a personal computer, tablet, thumb drive.
8. I WILL immediately report any lost or stolen device, personal or otherwise, that was used to access AHA systems to the Privacy Officer.
9. If I am permitted by my supervisor/manager to access Confidential Information remotely, I AM RESPONSIBLE for ensuring the privacy and security of such information at any location.
10. I WILL NOT take any pictures of patients for personal use with any device of any kind.
11. I WILL complete all required privacy and security training.
12. When my work or service at AHA ends, I WILL NOT disclose any Confidential Information, and I WILL NOT take any Confidential Information with me if I leave or I am terminated.
13. I UNDERSTAND that my access to Confidential Information and my UHCC e-mail account may be audited.
14. If I receive personal information through UHCC e-mail or other AHA systems, I AGREE that authorized AHA personnel may examine it, and I do not expect it to be protected by AHA.
15. I UNDERSTAND that AHA may remove or limit my access to AHA'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 AHA 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.: _____

Confidentiality Agreement

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

These are examples only. They do not include all possible breaches of confidentiality which may lead to disciplinary action.

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, 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.
- Sharing sensitive business information with a competitor.
- Emailing confidential information outside of AHA by unsecure methods (not encrypted).

Sharing your User ID and password:

- Sharing your password so a co-worker can log into AHA's computer system(s) to do their work or yours.
- Giving someone the access codes for employee files or patient accounts.

Leaving a secured application* unattended while signed on:

- Being away from your computer while you are logged into patient billing information, thereby allowing someone to access Confidential Information using your User ID and password.

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