

CONFIDENTIALITY AND USER ACCESS AGREEMENT

As a condition to my employment or relationship with Cambridge Health Alliance (“CHA”), I agree that at all times:

I WILL KEEP CHA INFORMATION AND ALL PATIENT INFORMATION CONFIDENTIAL.

- I will not disclose any patient or confidential CHA information (including any employee, financial, strategic or other information) in any way to anyone not associated with CHA unless I am authorized to do so.
- I will not access or disclose any patient or confidential CHA information to any co-worker or medical staff member except as needed to perform my duties or as is clinically necessary.
- I will keep all patient and confidential CHA information secure and will comply with all CHA policies about keeping this information secure. I understand that this applies to (1) all electronic information on computer systems and other electronic devices, (2) all paper records, and (3) all other forms of information. I will not discuss this information in places where it can be overheard. I will comply with all CHA policies on protecting all physical records (paper and any other device or thing on which information may be stored) from theft or disclosure.
- **I will not disclose any patient information or confidential CHA information after my employment or other relationship with CHA ends.**

I WILL COMPLY WITH ALL CHA POLICIES REGARDING ELECTRONIC INFORMATION AND THE USE OF CHA’S INFORMATION SYSTEMS.

- I will only email, electronically copy, or send patient information to destinations outside the CHA system as permitted by CHA’s privacy and information security policies. This includes sending information to or loading information onto any portable device such as a PDA, phone, or thumb drive.
- If I remotely access CHA’s computer system, I will not permanently save any patient or CHA information to any remote non-CHA computer. I will immediately delete any patient or CHA information that has been temporarily saved on any remote non-CHA computer.
- **I will keep all computer or system passwords strictly confidential and not disclose them in any way to anyone at any time or for any reason.**
 - I will physically secure any CHA password written on paper under lock and key.
 - I am responsible for all actions initiated via my log-in and password. I will not allow anyone else to use it to access any CHA device or system. I will take appropriate measures to ensure my password is not disclosed to others. I will log off of the system or lock the station I have been using when I have completed my tasks and any time I leave any computer unattended.
 - If my password is accidentally revealed, I will immediately contact my supervisor, the Help Desk, or the Chief Security Officer and request a new password. If I forget my password, I will contact the Help Desk.
- I will not download internet files onto my computer or open attachments from external emails, except for CHA business purposes. I will only download internet files from sites that I know or have reason to believe are legitimate sources.
- I will not install software of any kind without prior approval from the Information Technology department. I will not copy any CHA software without prior approval from the Information Technology department.

I UNDERSTAND THAT CHA MAY MONITOR MY COMPUTER AND TELEPHONE ACTIVITY.

- I understand the computer equipment, programs, and files I use in my job are CHA property and are made available to me solely for work-related use. I understand that CHA has the right to monitor my telephone use, my internet access, my email and all other information technologies systems to ensure such use is in compliance with CHA policies.
- I understand that my electronic signature will be used to track all of my transactions in certain systems.
- I acknowledge that CHA regularly copies electronic files (including email) to tape archives and that these files may be disclosed to third parties in certain circumstances.

IF I HAVE AUTHORIZED ACCESS TO CHA EMAIL ON MY PERSONAL PDA, I WILL COMPLY WITH THE FOLLOWING AT ALL TIMES:

I elect to have my CHA email synchronized to my personal PDA device. I understand and agree that CHA uses encryption software (MobileIron) to provide electronic security features for this process.

- I will not deactivate the PDA encryption software or the PIN feature on my PDA.
- I will promptly notify CHA if my personal PDA is lost or stolen such that CHA can perform a remote wipe of the data stored on the device.
- When accessing my CHA email on my personal PDA, I will comply with CHA's privacy and information security policies.
- **I UNDERSTAND THAT IF I DON'T COMPLY WITH ANY OF THESE SECURITY RULES, I MAY LOSE THE ABILITY TO ACCESS MY CHA ELECTRONIC MAIL ON MY PDA.**

I WILL REPORT ANY IMPROPER DISCLOSURE OF ANY PATIENT OR CHA INFORMATION AS SOON AS I LEARN ABOUT IT.

I understand failure to comply with this Agreement and CHA policies can result in formal disciplinary action, including termination of my CHA employment or immediate termination of my consulting or vendor agreement.

CLEARLY: print your full name here:	BELOW: You must provide accurate last-4-SSN, and accurate birth date, to ensure this document will be filed. Failure to do so may hold up access to any Information Technology computer accounts.
Your Signature:	Last-4-digits Social Security number (last-4 only):
Date signed:	Your Birthday (in format 1/1/1965):

THIS FORM WILL BE FILED WITH YOUR EMPLOYMENT OR CONTRACT RECORDS.

To the Manager:

Please fax all pages of this signed document to the Information Technology Department, User Access group at (fax to full 10-digit number):

617-507-7720

[DO NOT fax to in-house extension 7720]

No access, to any CHA systems, will be given out until this signed agreement is received by IT.

Revised: 3/17/2011