Applicant's Name: _____

Community Care Alliance
Procedure for BIDMC Information Technology Access

It is the responsibility of each Community Care Alliance (CCA) Community Health Center (CHC) to determine who, based on their job-related responsibilities, needs access to any or all of the following ITS functions at BIDMC: email, WebOMR Lite, and CCC (where available). The most limited access available allows a user to view patient information. It is therefore the responsibility of each CHC to train its staff members in the use of these systems and any limitations that should be imposed. BIDMC requires any individual who obtains an ITS log-in and password to complete a required on-line HIPAA training. If the training is not completed within a two week period, ITS access will be automatically terminated.

1. Each CCA CHC should have an identified , authorized contact person(s) – the signatory - to coordinate granting, monitoring, and terminating access to BIDMC ITS. Kelly McCarthy, Program Manager will maintain that list with IS Support.
2. The CCA/BIDMC Information Systems Request Form (page two of this document) and accompanying Confidentiality Acknowledgement must be completed, signed by the authorizing signatory from the community health center and applicant and faxed to BIDMC Identify Access Management at **617-754-8099** or emailed to **iam@bidmc.harvard.edu**.
3. For those staff seeking access to Trizetto Platform Services (TPS), a separate TPS Request form must be submitted. You do not need to submit this form for TPS Access.
4. For those staff also seeking access to WebOMR Lite, IT will forward any requests to the OMR Support Team. OMR Support will process within 24 hours of receiving access to WebOMR Lite. Order Entry access relies on the clinician (MD, NP or PA) being successfully credentialed at BIDMC.
5. The BIDMC Identity Access Management Team will contact the CHC signatory who in turn notifies the applicant. To access the new ITS account, the individual staff person must call IT to receive the Log-In and password--it will not be emailed. It is the responsibility of the individual to maintain his/her Log-In and password once received.
6. Individuals granted BIDMC ITS access will receive an email requiring them to complete the HIPAA Confidentiality Training within a specified time frame. If it is not completed within two weeks, access will be automatically terminated.
7. Individuals whose ITS accounts are dormant for 90 days are automatically terminated. To be reinstated, the BIDMC/CCA Information Systems Request Form must be completed and submitted again. The CHC administrator will be notified when access is reinstated.
8. CHCs may request regular audits of their employees' BIDMC ITS usage by emailing a listing of ITS users to CCA Program Manager.
9. It is the responsibility of the CHC to notify BIDMC IT or CCA when an employee with BIDMC ITS is no longer employed by the CHC or is terminated so that his/her ITS account may be disabled.

Questions should be directed to Kelly McCarthy at 617-667-6732, kmccart9@bidmc.harvard.edu or the Managing Director at 617-667-2602.

☐ **I have read and understand the Community Care Alliance Procedure for BIDMC Information Technology Access.**

_____ _____

Applicant's Signature **Date**

_____ _____

Authorized Site Manager/Designee Signature **Date**

Community Care Alliance

Beth Israel Deaconess Medical Center

Beth Israel Deaconess Medical Center
BIDMC/CCA Information Systems Request Form

All BIDMC/CCA IS Requests must be completed and signed by an Authorized Community Health Center contact. By default, users are granted the most restrictive level of access. All Accounts unused for 90 days or more will be disabled. Access can only be restored by completing this form. Requests will be processed within 3 business days of receipt.

FAX Request to 617-754-8099 or email: iam@bidmc.harvard.edu

TO BE COMPLETED BY REQUESTER (Pleas fill out form completely)

Date of Request**:**

TYPE OF REQUEST:

☐New Account ☐Disable Account ☐Re-enable Account ☐New Access ☐Other

ACCESS REQUEST

☐ITS Login ☐Dimock E-mail ☐WebOMR Lite ☐Other

APPLICANT'S INFORMATION:

Last Name: First Name:

Title: Department:

Date of Birth: SSN: (Last 4-digits ONLY)

Gender: ☐ Male ☐ Female

Employee Type: ☐Full Time ☐Part-Time ☐Per-Diem ☐Temp/Contract Employee
☐Intern ☐Other

Is the applicant a clinician/provider**?** ☐Yes ☐No

If the applicant is a NP or PA, who is the supervising physician:
Work Phone: Fax number:

Community Health Center: **South Cove Community Health Center**

TO BE COMPLETED BY: Authorized CHC Site Manager or other CHC designee

Last Name: _____ First Name: _____Title:_____

Email: _____Work Phone:_____

Signature: _____Date:_____

Note: Once processed, an email will be sent to the CHC contact, updating the status with additional instructions if needed.

CAREGROUP
HEALTHCARE SYSTEMS

CONFIDENTIALITY ACKNOWLEDGMENT

Any information learned during the performance of one's work at CareGroup or any of its affiliates (hereinafter "CareGroup") which is not commonly available to the public must be kept confidential. This applies to information about patients, employees, and medical staff, research, and business affairs. Further, this applies to information in any form - spoken, written or electronic.

Each individual working in the CareGroup environment is responsible for protecting the privacy of our employees, our staff, and our patients, and must take care to preserve confidentiality in conversations and in handling, copying, faxing, and disposing of documents. Unusual activity or behavior, which could threaten confidentiality, should be questioned and reported.

Access to CareGroup information is permitted only as required for the performance of one's job. For example, reading confidential information not directly required for job performance, even if that information is not further disclosed, is a violation of policy and is, therefore, strictly prohibited. All policies and procedures related to authorization and access to confidential information must be followed.

Only people with an officially granted account may access CareGroup computer systems and networks requiring passwords. Each person is responsible for maintaining confidentiality by never sharing passwords or access and by always locking or logging off a terminal or workstation when leaving the area. Each person is accountable for all activity occurring under his/her account, password, and/or electronic signature. Such activity may be monitored.

Disclosure of CareGroup confidential information is prohibited except when required for the performance of one's job for CareGroup and when specifically authorized. Disclosure of confidential information is prohibited indefinitely, even after termination of employment or business relationship, unless specifically waived in writing by an authorized party.

I certify that I have received and read this Confidentiality Acknowledgment and understand the requirements set forth in it. I understand that I will be subject to disciplinary action, up to and including termination of my employment, professional privileges, and business relationships, for violating CareGroup policies or failing to report violations of CareGroup policies.

Name: _____ Title: _____

_____ _____

Applicant Signature Date

Authorized Contact: _____ Title: _____

_____ _____

Authorized Contact Signature Date