BARNABAS HEALTH

POLICY # HIE-7

INFORMATION TECHNOLOGY AND SERVICES

POLICY

TITLE: **Access**

EFFECTIVE DATE: 6/18/2015

APPROVED BY:

System: Date: 9/1/2015

System Chief Information Officer/
Barnabas Health

ATTACHMENTS:

None

PURPOSE:

To ensure that only appropriate and specifically-authorized Authorized Users of registered Participants gain access to the BHIE.

POLICIES:

1. Access Control Responsibility and Management

    a. The BHIE will develop, disseminate, and periodically review/update the following:

        i. a formal, documented, access control policy that addresses, purpose, scope, roles, responsibilities, management commitment, coordination among Participants, and compliance, and

        ii. Implementation Procedures to facilitate the implementation of the access control policy and associated access controls.

    b. The BHIE will grant, manage and terminate access to the BHIE.

    c. Participants and Authorized Users shall cooperate and assist the BHIE as needed to ensure adequate access controls and management is implemented.

2. Access Request Process

a. Access to the BHIE must be restricted to Authorized Users and used only for Permitted Uses.

b. All Authorized Users must sign an Authorized User Agreement, or equivalent, as a prerequisite to obtaining access to the BHIE.

c. Business Associates of the BHIE are required to additionally execute a HIPAA compliant Business Associates Agreement.

d. If the request for access does not appear to be appropriate, discretion must be exercised before access is granted.

3. Role-Based & Task-Based Access

a. Access to the BHIE should be granted only to individuals with a legitimate need for access to the BHIE based upon roles (e.g., clinical care) and tasks (e.g., IT trouble shooting).

b. Access should be granted in accordance with role-based access matrices developed for the BHIE. Further approval may be needed if a request does not fit within the pre-approved role-based and task-based accesses.

4. Access Removal

Role-based access profiles may be removed or suspended from Authorized Users, at BHIE's sole discretion, for reasons including but not limited to:

a. Termination of Participant's participation in the BHIE;

b. Reported or detected misuse or abuse of access by an Authorized User;

c. Expiration of an Authorized User's job function or business need for access;

d. Change in Authorized User's job function; and

e. If directed by the BHIE Steering Committee.

5. Emergency Access

a. In general, emergency access to the BHIE is not permitted.

b. Exceptions may be made with the prior approval of the BHIE Steering Committee, and on a very limited case-by-case basis in certain circumstances.

6. User Credentials

a. Any person granted access to the BHIE shall have been assigned a user credentials, and will be asked to create his/her own password.

b. Audit trails of all sign-ons will be maintained by the BHIE.

c. If credentials are shared, disciplinary actions shall be taken, including in accordance with actions BHIE Policy 15 – Enforcement & Sanctions.

d. Authorized Users are not permitted to enter data under another person's credentials.

e. Authorized Users shall not allow another individual to log onto the BHIE using another's credentials.

f. If a potential breach is identified, steps shall be taken to secure the system.

7. Prohibited Access

a. Under no circumstances shall any Authorized User or Participant be considered permitted or authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the BHIE.

b. The list below is by no means exhaustive, but provides a framework for activities that fall into the category of prohibited access practices which are considered serious violations and may result in terminating an Authorized User from further access to the BHIE:

i. Revealing a BHIE account password to others or allow use of their account by any other individual for any reason;

ii. Using the BHIE for effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to accessing Data of which the Authorized User is not an intended recipient or logging into a server or account that the Authorized User is not expressly authorized to access;

iii. Circumventing user authentication or security of any server, network or account to access the BHIE;

iv. Copying, transmitting or providing information about the BHIE or any Data contained therein to any third party without proper authorization; or

v. Inappropriate reviewing of Data through the BHIE for an unauthorized purpose, or Prohibited Use.

QUALIFICATIONS: NA

EQUIPMENT: NA

PROCEDURE: NA

DOCUMENTATION: NA

INFECTION CONTROL: NA

SAFETY: NA

SECURITY OVERSIGHT GROUP (SOG) Approve for Release:

REFERENCES:

ORIGINAL DATE: 6/18/2015

REVIEWED DATE(S):

REVISED DATE(S):