BARNABAS HEALTH

POLICY # HIE-13

INFORMATION TECHNOLOGY AND SERVICES

POLICY

TITLE: **Security Incidents & Breaches of Unsecured Data**

EFFECTIVE DATE: 6/18/2015

APPROVED BY:

System: Date: 8/6/2015

System Chief Information Officer/
Barnabas Health

ATTACHMENTS:

None

PURPOSE:

To set forth minimum standards Participants and Authorized Users shall follow in the event of a Security Incident or Breach of Unsecured Data.

POLICIES:

1. Compliance with Law

Participants and their Authorized Users shall comply with the following, which are collectively the Breach Notification Laws:

a. HIPAA Breach Notification for Unsecured PHI (45 CFR Parts 160 and 164);

b. The New Jersey Identity Theft Prevention Act ("NJITPA"), N.J.S.A. 56:8-161 et seq.; and

c. NJITPA rules governing Written Security Programs, N.J.A.C. 13:45F-1.1 et seq., Subchapter 3.

Capitalized terms under this BHIE Policy shall have the same meanings given to such terms under the Breach Notification Laws, unless specified to the contrary.

2. Detecting Potential Breaches

    a. Each Participant shall strive to detect any circumstances that could lead to or result in a potential or actual Breach.

    b. As part of striving to detect Security Incidents and Breaches, Participant's systems shall be audited for evidence of Breaches in accordance with the BHIE Policy governing auditing.

3. Investigating Incidents and Breaches

    a. Participants shall investigate and evaluate any and all reports of internal Breaches (or potential security breaches).

    b. The applicable Participant/Barnabas Health affiliates' privacy officers, as appropriate, shall investigate reported and detected breaches that may affect another Participant of the BHIE. Such privacy officers shall consult with the BHIE Privacy Officer and BHIE Security Officer.

    c. Participants and the BHIE will adhere to the Breach Notification laws, in consultation with Barnabas Health Legal Affairs, when determining whether or not a Breach has occurred.

4. Reporting Obligations

    a. Any Participant that or Authorized User who has reason to believe that a Breach involving PHI or PI (under state law) has or may potentially occur with regard to another Participant's Data being accessed or disclosed through the BHIE must report such information to the applicable Participant/Barnabas Health affiliates' privacy officers, as appropriate, who shall then consult with the BHIE Privacy Officer and/or BHIE Security Officer, as appropriate.

    b. Notification shall be made in the most expedient time possible and without unreasonable delay.

    c. Initial notification of the Breach or potential Breach may be made to the BHIE Privacy Officer or BHIE Security Officer, as appropriate, by telephone hotline.

    d. Additional information to be included in any reports or third party notices shall be provided in writing.

5. Responsibilities in the Event of a Breach

    a. In the event of an actual or suspected Breach of unsecured PHI, either through notification by another Participant and Authorized User or otherwise, such Participant and Authorized User must, at a minimum:

i. In the most expedient time possible and without unreasonable delay, investigate (or, if the Participant is a Connected-HIE, then to require its applicable sub-network participant to investigate) the scope and magnitude of such actual or suspected Breach, and identify the cause of the Breach or potential Breach;

ii. **Mitigate** to the extent practicable, any harmful effect of such Breach that is known to the Participant. Participant's mitigation efforts shall correspond with and be dependent upon their internal risk analyses.

iii. Cooperate with Barnabas and any other Participants affected by the Breach to notify (or require the applicable Participant to notify) the Patient and any applicable regulatory agencies as required by and in accordance with applicable federal, state and local laws and regulations, including but not limited to the Breach Notification laws.

b. The BHIE may conduct its own investigation, which Participants and Authorized Users must cooperate with. This includes providing the results of the internal investigation, including the facts and circumstances surrounding the incident, and any action taken to mitigate harmful effects. Participants and Authorized Users must cooperate with each other, the BHIE Steering Committee and Administrator, and any applicable regulatory agencies, whether state or federal.

QUALIFICATIONS: NA

EQUIPMENT: NA

PROCEDURE:

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):