Policy: Number:

Applicability: Viewer, Provider, Receiver, Exchanger Effective: 9/23/2013

Policy:

Jersey Health Connect maintains minimum standards Participants and Authorized Users must follow in the event of a Security Incident or Breach, including reporting to the proper individuals as well as mitigating any harm that may arise from such Security Incident or Breach.

Procedure:

1) Compliance with Law

a) Participants and their Authorized Users shall comply with the following:

i) § 13402 of the Health Information Technology for Economic and Clinical Health Act ("HITECH) Act, and specifically (the "Breach Statute");

ii) HHS Final Rule for Breach Notification for Unsecured PHI (45 CFR Parts 160 and 164, Subpart D) (the "Breach Notification Rule");

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

iv) NJITPA rules governing Written Security Programs, N.J.A.C. 13:45F-1.1 et seq., Subchapter 3 (the "NJITPA Breach Rule").

b) Capitalized terms under this JHC 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) Participants shall develop policies and procedures for monitoring all activities and circumstances that could lead to or result in a potential or actual Breach.

b) Participants or Authorized Users who have or should reasonably have reason to believe that a Breach involving PHI or PI (under state law) has or may potentially have occurred with regard to another Participant's Data being accessed or disclosed through Jersey Health Connect must report such information promptly and without unreasonable delay to the JHC Administrator.

c) Participants shall require all BAs to promptly and without unreasonable delay, but in no case later than thirty (30) days, report an actual or suspected

Security Incident or Breach to the Participant. Participants shall require such reports even if a BA's investigation concludes that no Security Incident or Breach occurred.

d) As part of striving to detect Security Incidents and Breaches, Participant systems shall be audited for any evidence of unauthorized acquisitions, access, uses, or disclosures of PHI or PHI in accordance with the JHC Policy governing Auditing.

e) Jersey Health Connect shall be responsible for such auditing and shall immediately inform JHC's Privacy Officer and Security Officer in the event of an actual or constructive discovery of such incidents, and/or upon identification of system gaps or inadequate safeguards.

3) Investigating Incidents and Breaches

a) Participants shall promptly and without unreasonable delay investigate and evaluate any and all reports of internal Breaches (or potential security breaches). This shall include actual or suspected Security Incidents or Breaches that occurred within a Business Associate.[i]

b) The Privacy and Security Officer shall investigate reported Breaches that may affect another Participant of or occur through Jersey Health Connect.

c) Participants and Jersey Health Connect will adhere to the Breach Notification laws when assessing whether or not a Breach has occurred under federal or State law.

4) Reporting Obligations [ii]

a) Participants and Authorized Users must notify Jersey Health Connect in the event that they become aware of any actual or suspected Security Incident or Breach of unsecured PHI accessed through Jersey Health Connect.

b) For Participant HIOs, the HIO shall additionally notify each of its own Participants that may have been affected by the actual or suspected Breach.

c) Participants shall notify Patients who may have been affected by the actual or suspected Breach in compliance with the Breach Notification laws, as well as any applicable regulatory agencies as required by federal, state and local laws and regulations including HIPAA, HITECH and NJITPA.

d) Initial notification of the incident, Breach, or potential Breach may be made to Jersey Health Connect's Privacy Officer by telephone. Additional information to be included in any reports or third party notices shall be provided in writing.

e) All Notification required by this JHC Policy and under the Breach Notification laws and regulations shall be made in the most expedient time possible, without unreasonable delay, and within any required time periods.

5) Responsibilities in the Event of a Breach.

a) Participant Obligations. Participants must develop and implement a Breach plan as part of their HIPAA policies and procedures. The plan shall provide that, in the event the Participant or any of its Authorized Users or BAs becomes aware of any actual or suspected Breaches of unsecured PHI, either through notification by another Participant and Authorized User or otherwise, such Participant and Authorized User must, at a minimum:

i) Notify the Privacy and Security Officer regarding the Breach or potential Breach;

ii) 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 root cause of the Breach or potential Breach;

iii) 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.

iv) Cooperate with Jersey Health Connect 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 HITECH and New Jersey's breach notification law.

v) Impose and document Sanctions where appropriate and in accordance with the JHC Enforcement & Sanctions Policy.

vi) Retain Documentation related to Breach incidents in a Security Incident/Breach Log, including, but not limited to, reports, investigations, evaluations, notices, sanctions and other corrective action taken, for a period of at least six (6) years from the date of the incident.

b) Jersey Health Connect Obligations.[iii]

i) Jersey Health Connect shall immediately respond to, evaluate, and investigate any and all reported actual or suspected Breaches involving PHI or PHI that may affect Patients and Participants within the timeframes as set forth in the applicable HIPAA BAAs between Jersey Health Connect and the Participants.

ii) Jersey Health Connect shall investigate such reports in accordance with these HIE Policies.

iii) Jersey Health Connect shall cooperate and coordinate with the affected Participant(s) to:

(1) Investigate the scope, magnitude and harm of the actual or suspected

Breach;

(2) Mitigate to the extent practicable the harm that may have occurred to Jersey Health Connect and other Participants;

(3) Reevaluate Safeguards to identify and address any system security gaps;

(4) Impose Sanctions upon Participants and/or Authorized Users where appropriate and in accordance with the JHC Enforcement & Sanctions Policy.

Revision History:
3/12/2012 New Policy
9/13/2013 Revised Effective 9/23/2013

---

[i] New Jersey Health Information Network (NJHIN) Security Policy and Procedure 3.5, "Incident and Breach" **ALSO** requires Members/Participants to **designate an individual with authority** to determine whether an incident is or is not a breach.

[ii] NJHIN Security Policy and Procedure 3.5 also requires Members/Participants to **report actual or suspected Breaches to the NJHIO** in the most expedient time possible and without unreasonable delay, in writing.

[iii] NJHIN Security Policy and Procedure 3.5 also requires NJHIOs to **develop an incident management and breach plan**, and respond to reported security incidents and breaches through specific Member/NJHIO notification, investigation and mitigation, as well as sanctions.