Policy: Security Risk Assessment Number: 7

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

Policy:

Jersey Health Connect shall routinely assess potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI maintained by Jersey Health Connect and the implementation of necessary security measures.

Procedure:

1) Risk Assessment
   a) *JHC Responsibilities.*
      i) Jersey Health Connect shall implement administrative, physical and technical safeguards as appropriate to protect the confidentiality, integrity, availability of electronic PHI and other Data created, received and maintained in Jersey Health Connect.
      ii) Jersey Health Connect shall implement processes and procedures for formally identifying and assessing potential risks and vulnerabilities ("Risk Assessment") of all systems and applications through which electronic PHI and other Data is maintained and transferred by JHC.[1]
      iii) Jersey Health Connect shall document its Risk Assessment processes and procedures.
      iv) Such Risk Assessment must be performed at least once every three years or within a shorter period of time the Jersey Health Connect Board may otherwise determine is appropriate.
      v) Upon a significant change in the Jersey Health Connect environment, systems and/or applications, a Risk Assessment shall be performed by Jersey Health Connect. Such changes may include, but are not limited to:
         (1) Introduction of new systems;
         (2) Significant upgrades to, or retirement of, systems;
         (3) Physical relocation of IT assets;
         (4) Reorganization of Jersey Health Connect's organizational structure;
         (5) Occurrence of a Security Breach or incident.

[1] 45 CFR 164.308(a)(1).

vi) In connection with the aforementioned processes and procedures, Jersey Health Connect shall maintain a complete and accurate inventory of all systems which store, process and transmit electronic PHI.

vii) In performing a Risk Assessment, JKHC shall at a minimum:

(1) Assess the scope of the Risk Assessment;

(2) Gather appropriate Data;

(3) Identify criticality of systems, applications and Data;

(4) Identify and document potential threats and potential vulnerabilities in systems, applications and Data;

(5) Assess current security measures, such as, but not limited to, current Access controls and whether additional Access controls are reasonably necessary to mitigate potential risks;

(6) Determine the likelihood of a threat occurrence that would trigger a vulnerability and the potential impact of such threat occurrence;

(7) Determine levels of risk, such as through use of a Risk Level Matrix;

(8) Identify plans for corrective action and security measures that may be necessary as well as to mitigate risks identified by the Risk Assessment;

(9) Document results of the Risk Assessment.

viii) Jersey Health Connect shall at all times comply with the general requirements, standards, implementation specifications, and maintenance requirements of the HIPAA Security Rule for information security.

2) Participant and Authorized User Responsibility.

a) Participants are responsible for developing and implementing policies and procedures for performing Risk Assessment to assess the potential risks and vulnerabilities unique to their respective networks and systems through which electronic PHI from and to Jersey Health Connect is transferred.[2]

b) Such Risk Assessment must be performed at least every three years or within a shorter period of time the Participant may otherwise determine is appropriate.

c) Upon a significant change in a Participant's environment, systems and/or applications, each Participant shall be responsible for completing a Risk Assessment. Such changes may include, but are not limited to:

i) Introduction of new systems;

ii) Significant upgrades to, or retirement of, systems;

iii) Physical relocation of IT assets;

iv) Reorganization of organizational structure;

[2] 45 CFR 164.308(a)(1).

v) Occurrence of an actual or suspected Security Incident or Breach.

d) Participants and Authorized Users shall formally document Risk Assessment processes and procedures, including identifying all systems which store, process and transmit electronic PHI and the physical location of IT assets.

e) In performing a Risk Assessment, Participants shall be responsible for:

i) Assessing the scope of the Risk Assessment;

ii) Gathering appropriate Data;

iii) Identifying criticality of systems, applications and Data;

iv) Identifying and documenting potential threats and potential vulnerabilities in systems, applications and Data;

v) Assessing current security measures, such as, but not limited to, current Access controls and whether additional Access controls are reasonably necessary to mitigate potential risks;

vi) Determining the likelihood of a threat occurrence that would trigger a vulnerability and the potential impact of such threat occurrence;

vii) Determining levels of risk, such as through use of a Risk Level Matrix;

viii) Identify plans for corrective action and security measures that may be necessary as well as to mitigate risks identified by the Risk Assessment;

ix) Document results of Risk Analysis.

f) Participants and Authorized Users shall submit to and cooperate with Jersey Health Connect in connection with Jersey Health Connect's performance of Risk Assessment in accordance with this Jersey Health Connect Policy and the HIPAA Security Rule and other applicable federal and state laws.

g) Participants and Authorized Users shall at all times comply with the general requirements, standards, implementation specifications and maintenance requirements of the HIPAA Security Rule for information security and the minimum Security requirements set forth in the HIE Participation Agreement, Schedule 10.3.

3) Auditing for Compliance

a) Processes and procedures shall be developed for auditing compliance by Participants and Authorized Users with this Jersey Health Connect Policy and in accordance with the JHC Auditing Policy.

b) Participants and Authorized Users shall submit to and cooperate with such auditing performed by Jersey Health Connect to ensure compliance with this Jersey Health Connect Policy and the HIPAA Security Rule and other applicable federal and state laws.

c) Sanctions for noncompliance with this Jersey Health Connect Policy and the applicable laws and regulations shall be imposed in accordance with the JHC "Enforcement & Sanctions" Policy by Jersey Health Connect and/or Participants, as may be appropriate.

4) Third Party Vendors – all third party vendors, such as the PHR Vendor, shall be required to comply with this Policy and additionally follow the Risk Management Framework standards and guidance set forth by NIST Special Publication 800-66 Revision 1 for compliance with the HIPAA Security Rule.

Revision History:

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