Policy: Nationwide Privacy and Security Framework Number: 1

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

Policy:

The Office of National Coordinator (ONC) for Health Information Technology published the *Nationwide Privacy and Security Framework for Electronic Exchange of IIHI* ("the Framework"), which is developed for the primary purpose of establishing a single, consistent approach to address the privacy and security challenges related to electronic health information exchange through a network.

The Framework includes **eight (8) guiding principles** that establish the roles of individuals and the responsibilities of those who hold and exchange electronic individually identifiable health information (IIHI) through a HIE network (the "Guiding Principles").

In connection with each Guiding Principle, ONC provides further details and explanation with regard to what the principle is designed to do, and its parameters (each, a "Detail" and collectively, the "Details"). Jersey Health Connect's HIE Policies have been developed around the ONC's Guiding Principles and their corresponding Details.

In connection with the development, input was obtained in from Jersey Health Connect's Board, members of JHC Committees, including participants of the Legal and Policy Committee, Technology Committee, and Executive Committee, as well as input from initial participating members. However, because federal and state law and policy regarding electronic health information exchange is evolving rapidly, revisions to these HIE Policies is anticipated and will be undertaken as needed to align such policies with changes to existing laws and standards.

The Guiding Principals and Details are:

1) Openness & Transparency
   a) There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their IIHI.
   b) Individuals should be able to understand what IIHI exists about them.
   c) Individuals should be able to understand how their IIHI is collected, used, and disclosed.
   d) Individuals should be able to understand whether and how they can exercise choice over such collections, uses, and disclosures.

e) Persons and entities that participate in a network for the purpose of electronic exchange of IIHI should provide reasonable opportunities for individuals to review who has accessed their IIHI or to whom it has been disclosed, in a readable form and format.
f) Notice of policies, procedures, and technology— including what information will be provided under what circumstances — should be timely, and, wherever possible, made in advanced of the collection, use, and/or disclosure of IIHI.

2) Individual Choice
   a) Persons and entities that participate in a network for the purpose of electronic exchange of IIHI should provide reasonable opportunities and capabilities for individuals to exercise choice with respect to their IIHI.
   b) The degree of choice made available may vary with the type of information being exchanged, the purpose of the exchange, and the recipient of the information.
   c) Applicable law, population health needs, medical necessity, ethical principles, and technology, among other factors, may affect options for expressing choice.
   d) Individuals should be able to designate someone else, such as a family member, care–giver, or legal guardian, to make decisions on their behalf.
   e) When an individual exercises choice, the process should be fair and not unduly burdensome.
3) Collection, Use & Disclosure Limitation
   a) IIHI should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s).
   b) Appropriate limits should be established on the type and amount of information collected, used, and/or disclosed.
   c) Persons and entities should take advantage of technological advances *to limit data collection, use, and/or disclosure.*
   d) IIHI should never be collected or used to discriminate against an individual.
4) Safeguards
   a) IIHI should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
   b) Persons and entities that participate in a network for the purpose of electronic exchange of IIHI should implement administrative, technical, and physical safeguards to protect information, including assuring that only authorized persons and entities and employees of such persons or entities have access to IIHI.
   c) These safeguards should be developed after a thorough assessment to determine any risks or vulnerabilities to IIHI.
   d) Administrative, technical, and physical safeguards should be reasonable in scope and balanced with the need for access to IIHI.
5) Data Quality & Integrity
   a) Persons and entities that participate in a network for the purpose of electronic exchange of IIHI have a responsibility to maintain IIHI that is useful for its intended purposes, which involves taking reasonable steps to ensure that information is accurate, complete, and up–to–date, and has not been altered or destroyed in an unauthorized manner.

b) Persons and entities have a responsibility to update or correct IIHI and to provide timely notice of these changes to others with whom the underlying information has been shared.
c) Moreover, persons and entities should develop processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, IIHI.

6) Correction
   a) Individuals should be provided with practical, efficient and timely means to dispute the accuracy or integrity of their IIHI.
   b) Individuals should be provided with practical, efficient and timely means to have their IIHI corrected.
   c) Individuals should be provided with a timely means to have the correction or dispute communicated to others with whom the underlying information has been shared.
   d) Individuals should be provided with a timely means to have a dispute documented if their requests are denied.
7) Accountability
   a) Mechanisms for assuring accountability of persons and entities that participate in a network for the purpose of electronic exchange of IIHI, should address monitoring for internal compliance including authentication and authorizations for access to or disclosure of IIHI.
   b) Mechanisms for assuring accountability of persons and entities that participate in a network for the purpose of electronic exchange of IIHI, should address the ability to receive and act on complaints, including taking corrective measures.
   c) Mechanisms for assuring accountability of persons and entities that participate in a network for the purpose of electronic exchange of IIHI, should address the provision of reasonable mitigation measures, including notice to individuals of privacy violations or security breaches that pose substantial risk of harm to such individuals.
8) Individual Access
   a) Individuals should be provided with a simple and timely means to access and obtain their IIHI in a readable form and format.
   b) Individuals should be able to obtain this information easily, consistent with security needs for authentication of the individual.
   c) Such information should be provided promptly so as to be useful for managing their health.
   d) Additionally, the persons and entities that participate in a network for the purpose of electronic exchange of IIHI should provide such information in a readable form and format, including an electronic format, when appropriate. In limited instances, medical or other circumstances may result in the appropriate denial of individual access to their health information.

Revision History:

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