Policy: Definitions Number: 2

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

DEFINITIONS

Terms used but not otherwise defined in these Jersey Health Connect (JHC) Health Information Exchange (HIE) Policies shall have the meanings ascribed to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended (the "HIPAA Statute"), and its related "Privacy Rule" (45 CFR Parts 160 and 164, Subpart E), "Security Rule" (45 CFR Part 160 and 164, Subpart C), and "Breach Rule" (45 CFR Part 160 and 164, Subpart D) promulgated by the Secretary of Health and Human Services ("HHS") (collectively, the HIPAA Statute, the Privacy Rule and the Security Rule and are refereed to, hereinafter, as "HIPAA"), all as amended by the Health Information Technology for Economic and Clinical Health Act enacted on February 17, 2009 (the "HITECH Statute"), and any regulations promulgated thereunder (collectively, the "HITECH Rules," and together with the HITECH Statute, referred to hereinafter as "HITECH"), as well as any other applicable laws concerning the privacy and security of health information.

The following terms shall have the following definitions:

1.1 "Approval" or "Assent" may include, for purposes of JHC and when required under an applicable law from a Patient before Data can be disclosed, the Patient's signed Acknowledgment of receipt of a Health Care Provider's HIPAA Notice of Privacy Practices setting forth permissible uses and disclosures of the Patient's Protected Health Information, unless and until the Patient has effectively "opted-out" of JHC in accordance with JHC's opt-out procedures.

1.2 "Authorized User" means an individual who is also a registered Participant, or an individual designated to use the Services on *behalf of* an approved and authorized JHC Participant, including a Participant that has been granted access rights to the JHC Network.

1.3 "Authorized User Agreement" means a legally-binding agreement with an individual designated by a Participant as an Authorized User pursuant to which such

individual agrees to comply with the terms and conditions set forth in such agreement, and the JHC Polices.

1.4 "Data" means information provided to or through the JHC Network, including Protected Health Information (PHI) and Individually Identifiable Health Information (IIHI), as defined under HIPAA, and any other information that identifies a patient and is provided to or through JHC.

1.5 "Data Exchange" means electronically providing or accessing Data through JHC.

1.6 "Data Receiver" means an organization, such as a hospital, physician practice, clinical laboratory, pharmacy, governmental agency or other entity, that has entered into an agreement allowing them to *receive* Data that is Pushed through JHC and into such Data Receiver's electronic medical record (EMR) or other similar Data-collection repository, or is specifically made available to such Data Receiver for limited viewing. A Data Receiver also may, but is not required to be a Data Supplier. A Data Receiver is not authorized to access Data directly from the JHC network unless such Data Receiver is registered as a Data Exchanger.

1.7 "Data Exchanger" means an organization, such as a hospital, physician practice or other eligible entity, that has registered and entered into a Participation Agreement (or an equivalent) and will, in accordance with the terms of such agreement, these HIE Policies and applicable law, make Data *available for access* by other Participants through JHC and also has the authority to directly access and Pull Data from JHC that is made available by other Participants. A Data Exchanger is both a Data Supplier and Data Receiver.

1.8 "Data Supplier" means an organization, such as a hospital, physician practice, clinical laboratory, pharmacy claims aggregation company, governmental agency or other entity, that has entered into a binding agreement and will, in accordance with the terms of such agreement, these HIE Policies and applicable law, transmit Data to JHC and make it *available for access* by authorized Participants through JHC. A Data Supplier may also be a Data Receiver; however a Data Supplier shall not have authority to fully access and Pull Data through JHC, unless such Participant is registered as a full Data Exchanger.

1.9 "Electronic Health Record" or "EHR" means a Patient's collective or aggregated "record" of information comprised of information contributed to such EHR from source electronic medical record (EMR) systems maintained by Health Care Providers.

1.10 "Electronic Medical Record" or "EMR" means an electronic system used to enter, maintain and store patient clinical information, including such information as required

under applicable state law and federal regulations, and maintained by a single Health Care Provider who, for purposes of these HIE Policies, is a Participant of JHC.

1.11 "Health Care Provider" means a physician, group practice, hospital or health system, clinical laboratory, or other health care organization or professional that provides treatment to Patients. In connection with JHC, each Health Care Provider will be either a Data Supplier or Data Receiver (or both), or a Data Exchanger, as well as a Participant (entity-level) or Authorized User (user-level).

1.12 "Health Information Exchange" or "HIE" means the electronic exchange of patient information between Health Care Providers or entities through a secure network and processes that complies with federal and state standards for privacy and security.

1.13 "Health Information Organization" or "HIO" means the entity established to oversee and manage the operations of its participants for purposes of providing coordinated and networked Health Information Exchange. For purposes of these HIE Policies, Jersey Health Connect is an HIO.

1.14 "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 (HIPAA) collectively with the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E ("Privacy Rule"), and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C ("Security Rule"), as amended by the Health Information Technology for Economic and Clinical Health Act and regulations promulgated thereunder (collectively, "HITECH").

1.15 "Implementation Procedures" shall mean any written procedures developed by JHC to provide more specific processes for implementing an HIE Policy. Implementation Procedures shall be made available to all Participants of JHC.

1.16 "Joinder Agreement" means the agreement that makes a new applicant individual or entity a Party to certain or all of the provisions contained within the signed Participation Agreement between the JHC Founding Hospital Members and subject to the terms and conditions of such Agreement, and any additional terms and conditions as may apply to the respective individual or entity.

1.17 "Participant" means, in general, an entity that has entered into a binding agreement with Jersey Health Connect setting forth the terms and conditions of access to and use of the JHC Network after such entity is approved as an authorized Participant of JHC, and shall include, upon registration and approval, each Founding Hospital Member listed as a signatory on the Founding Hospital Member Participation Agreement. All new entities seeking to participate with JHC (i.e., an "applicant") shall not be granted the right to access or participate in JHC as a

Participant until such applicant has executed a "Participation Agreement" or "Joinder Agreement" and the applicant is approved as an authorized Participant.

1.18 "Participant User Type" shall mean the category of Participants to which a particular applicant is assigned based upon that its relationship to the JHC Network and other Participants, and includes classification of such Participant as either a Data Supplier, Data Receiver, or Data Exchanger.

1.19 "Participation Agreement" means the binding agreement that all Participants of JHC are required to enter in to and which sets forth the terms and conditions of access to and use of the JHC Network, Services and Data and compliance with the HIE Policies and the HIE vendor's Terms of Use. The Participation Agreement shall be in substance identical to that executed by the Founding Hospital Members, and may be satisfied by execution of a "Joinder Agreement"

1.20 "Patient" means an individual who has received or will receive treatment or health care services from a Health Care Provider.

1.21 "Permitted Use(s)" shall mean the permitted purpose(s) for which Data received through JHC may be accessed and used, as more particularly set forth in these HIE Policies. Any use of Data that is not set forth as a Permitted Use under the HIE Policies shall be, for purposes of JHC, considered a Prohibited Use.

1.22 "Personal Health Record" or "PHR" means an electronic, universally available, resource of health information that may originate from either a Health Care Provider or the Patient, but is controlled and managed exclusively by the Patient.

1.23 "Prohibited Use(s)" shall mean any access or use of Data through JHC for any reason or purpose other than a Permitted Use. Prohibited Uses may include, but are not necessarily limited to, manipulating, aggregating, integrating, compiling, merging, reorganizing, regenerating, transferring or otherwise using or disclosing Data for any purpose except for treatment and such other Permitted Uses specifically allowed for in accordance with the JHC Polices.

1.24 "Pull" shall mean, with regard to JHC and/or an applicable technological application, that Data maintained in JHC may be accessed, viewed, copied, and "pulled" for a Permitted Use into a Participant's EMR or other similar repository by an Authorized User.

1.25 "Push" shall mean, with regard to JHC and/or an applicable technological application, that Data residing within a Participant's EMR is either automatically "contributed to" the JHC centralized EHR based upon pre-established rules, or the Participant elects to send Data to JHC.

1.26 "Registration" means the process pursuant to which an entity or individual is registered as a Participant or Authorized User of JHC, and in accordance with an executed Participation Agreement or Authorized User Agreement, as applicable.

1.27 "State Law" shall mean the laws of the State of New Jersey, unless specifically stated otherwise in these HIE Policies or an agreement with the applicable Participant.

1.28 "Jersey Health Connect, a New Jersey Non-Profit Corporation", or "JHC" means the entity that was incorporated in 2010 for the purpose of establishing, operating, maintaining and conducting a regional health information organization. It includes the technological and operational infrastructure that facilitates the authorized and secure location, access and sharing of Data, including Patients' health, demographic and related information, held by multiple Health Care Providers by allowing registered Participants' Authorized Users to authenticate and communicate securely over an entrusted network for access and exchange of such Data.

1.29 "JHC Executive Director" shall mean the individual in the role designated by JHC Board to perform certain administrative and other day-to-day functions with regard to JHC. The JHC Executive Director.

1.30 "JHC Board" shall mean the governing and decision-making body for JHC, as further described in these HIE Policies and the JHC Bylaws.

1.31 "HIE Policies" shall mean the policies and procedures approved by JHC Board, as may be amended from time-to-time, that apply to and must be complied with by each and all registered Participants and Authorized Users of JHC.

1.32 "JHC Privacy Officer" or "Privacy Officer" shall mean the individual responsible for overseeing JHC's compliance with the privacy requirements under HIPAA, HITECH and other applicable privacy laws. The JHC Privacy Officer shall be the primary contact for all notifications regarding potential or actual privacy violations in connection with JHC.

1.33 "JHC Security Officer" or "Security Officer" shall mean the individual responsible for overseeing JHC's compliance with security requirements under HIPAA, HITECH and other applicable security laws. The JHC Security Officer shall be the primary contact for all notifications regarding potential or actual security violations in connection with JHC.

Revision History:

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