JERSEY Health Connect
Connecting your healthcare needs

HEALTH INFORMATION EXCHANGE POLICIES

Policy: Authorization and Access Number: 8

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

Policy:

Jersey Health Connect forbids unauthorized access to information and must maintain Data integrity and quality. This Policy shall set forth standards for verifying and authenticating the identity and the authority of an Authorized User requesting Data through Jersey Health Connect. This Policy also sets forth requirements for Patient access to PHRs.

Procedure:

1) Access Control Responsibility and Management[i]

a) Jersey Health Connect and its HIE Vendor shall be responsible for developing, disseminating, and periodically reviewing/updating the following:

i) A formal, documented access control policy that addresses, purpose, scope, roles, responsibilities, management commitment, coordination among Participants, and compliance; and

ii) Implementation Guidelines to facilitate the access control policy and associated access controls.

b) JHC's HIE Vendor shall be responsible for *managing* access control for Jersey Health Connect.

c) Participants and Authorized Users shall cooperate and assist Jersey Health Connect as needed to ensure adequate access controls and management is implemented.

d) The HIE Vendor shall be responsible for developing and managing authentication and access of Patients and their authorized representatives to the respective PHRs. Participants and their Authorized Users shall cooperate and assist as needed.

2) HIE Access Request Process

a) Participants may request certain employees, agents and contractors be approved for access to Jersey Heath Connect as Authorized Users. Access to Jersey Health Connect <u>must</u> be restricted to Authorized Users.

b) All Authorized Users <u>must</u> sign an Authorized User Agreement, or equivalent, as a prerequisite to obtaining access to Jersey Health Connect in

accordance with the JHC Participants & Authorized Users Policy and Procedures.

c) Participants are required to additionally execute a HIPAA & HITECH-compliant Business Associate Agreement with all Business Associates.

d) Identity-proofing procedures shall be implemented that require Authorized Users to provide identifying materials and information upon application for access to Jersey Health Connect. Each Participant shall be responsible for confirming the identity, credentials and authority of each Authorized User Participant wishes to access the JHC. Once approved by Jersey Health Connect as an Authorized User, all individuals seeking to access Jersey Health Connect shall also be authenticated in accordance with the JHC Authentication Policy.

e) If the request for access does not appear to be appropriate, Jersey Health Connect may decline the request in its sole discretion.

3) Role-Based & Task-Based Access [ii]

a) Access to Jersey Health Connect shall be granted only to individuals with a legitimate need for access to Jersey Health Connect based upon roles (e.g., clinical care) and tasks (e.g., IT trouble-shooting).

b) Access should be granted in accordance with matrices developed for Jersey Health Connect. Further approval, which may be granted or denied at the sole discretion of Jersey Health Connect, may be needed if a request does not fit within the pre-approved role-based and task-based accesses.

4) Access Removal [iii]

a) Role-based access profiles must be removed or at least temporarily suspended from Authorized Users for reasons including but not limited to:

i) Termination of Participant's participation in Jersey Health Connect;

ii) Reported or detected misuse or abuse of access by an Authorized User;

iii) Expiration or termination of an Authorized User's job function or business need for access;

iv) Change in Authorized User's job function; and

v) When directed by the Jersey Health Connect Board, in its sole discretion.

b) Participants are responsible for immediately notifying JHC in the event an Authorized User's role-based access must be removed, suspended or modified based on changes to the Authorized User's professional status (i.e., suspension or termination of professional license and/or revocation or change in clinical privileges).

5) Emergency Access

a) In general, emergency access to Jersey Health Connect is permitted for all patients who have *not* opted-out of JHC.

b) If a patient has opted-out of JHC, then the patient's Data in JHC may in the event of an emergency.

6) Password and Log-in Controls [iv]

a) Authorized Users granted access to Jersey Health Connect shall be assigned a "password" and unique identification number or username and other security mechanisms as determined and issued by JHC and/or its designee.

b) Authorized Users shall be informed and trained on:

i) Selecting a strong password;

ii) Not sharing or posting passwords;

iii) Not writing down their password and placing it at or near the terminal.

c) Authorized Users are prohibited from allowing another individual to log onto Jersey Health Connect using another's personal password or unique ID or permit another person to log on with their personal password or unique ID.

d) Authorized Users shall not allow another individual to enter Data in Jersey Health Connect under their unique ID nor enter Data in Jersey Health Connect using the unique ID of another individual.

e) Automatic log-off from Jersey Health Connect shall occur after a certain period of idle time.

f) Audit trails of all Authorized User log-ins, log-in attempts, and Data accessed shall be maintained in compliance with the JHC Auditing Policy.

g) Compliance with this HIE Policy shall be strictly enforced. Disciplinary action must be taken by Participants and/or Jersey Health Connect in accordance with the HIE Enforcement & Sanctions Policy as may be appropriate in response to violations of this policy.

h) If an actual or potential Breach is identified by a Participant, Authorized User and/or Jersey Health Connect, steps shall be taken to secure the system in accordance with the JHC Security Incidents & Breaches Policy.

7) Prohibited Access

a) Under no circumstances is any Authorized User or Participant permitted or authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Jersey Health Connect.

b) The list below is by no means exhaustive, but provides a framework for activities that fall into the category of *prohibited access* practices which are considered serious violations and may result in terminating an Authorized User from further access to Jersey Health Connect:

c) Revealing a Jersey Health Connect password to others or allow use of their account by any other individual for any reason;

d) Using Jersey Health Connect for effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to accessing Data of which the Authorized User is not an intended recipient or logging into a server or account that the Authorized User is not expressly authorized to access;

e) Circumventing user authentication or security of any server, network or account to access Jersey Health Connect;

f) Copying, transmitting or providing information about Jersey Health Connect or any Data contained therein to any third party without proper authorization; or

g) Inappropriate review of Data through Jersey Health Connect for an unauthorized purpose or Prohibited Use, such as accessing co-worker PHI to harass or intimidate, or collecting information regarding another Participant's practices.

8) PHR Access.

a) PHR Vendor Responsibilities.

i) *Authorization and Access Credentials* – The PHR Vendor shall follow commercially reasonable guidelines and best practices in identifying materials and proofs which will be required prior to enrolling a Patient or his or her personal representative in the PHR system. Access credentialing mechanisms shall include, at a minimum:

(1) Assigning of unique usernames and passwords

(2) Automatic log-off mechanisms

(3) Audit trails for Patient/personal representative and other accesses to the PHR system

(4) Mechanisms for detecting, preventing and responding to unauthorized accesses or attempts to access Patient PHRs.

ii) *Authentication* – The PHR Vendor shall comply with the minimum standards set forth by the JHC Policy "Authentication" for verifying and authentication of Patients and their authorized representatives.

b) *Limiting of Electronic Identifiers by PHR Vendor* - The PHR Vendor shall follow commercially reasonable guidelines and best practices in limiting the release or exposure of information that can be directly or indirectly tied to a Patient while such Patient or his or her personal representative is authenticating and accessing his or her PHR, including but not limited to IP addresses, cookies and web beacons.

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 3.1, "Authorization." This policy and procedures requires NJHIOs to set forth (i) categories of Authorized Users; (ii) define purposes for which Authorized Users in those categories may access PHI via the NJHIN; and (iii) define the types of PHI that Authorized Users may access (e.g., demographic data only, clinical data).

[ii] NJHIN Security Policy and Procedure 3.1 sets forth specific categories of Authorized Users and the purposes for which access to specified types of information may be granted by NJHIOs. See also NJHIN Security Policy and Procedure 3.3, "Access."

[iii] NJHIN Security Policy and Procedure 3.3 also requires termination of access and other sanctions to redress policy or procedural violations.

[iv] NJHIN Security Policy and Procedure 3.3, "Access." This policy and procedures requires NJHIOs to implement minimum access controls governing when and how a patient's information may be accessed by an NJHIO Member (JHC Participant). See also NJHIN Security Policy and Procedure 3.2, "Authentication."