JERSEY Health Connect
Connecting your healthcare needs

HEALTH INFORMATION EXCHANGE POLICIES

Policy: Authentication | Number: 9

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

Policy:

Jersey Health Connect requires Participants to set minimum standards for authentication of its Authorized Users prior to their accessing Jersey Heath Connect.

Procedure:

1) Minimum Authentication Standards [i]

a) Each Participant shall be responsible for following best practices for authentication requirements to verify and authenticate the identity of its Authorized Users who shall have access to Data through Jersey Health Connect.

b) Authorized Users shall be uniquely identified and authorized in accordance with the JHC Authorization and Access Controls Policy before they may be granted access to Jersey Health Connect.

c) Specific sensitive devices, such as those providing data to the PHR, shall be identified and authenticated before establishing a connection to Jersey Health Connect.

d) Additionally, all Authorized Users shall be authenticated before given access to any resource containing Patient Data. Such authentication shall be implemented using an authentication methodology that meets the minimum technical requirements for Authentication Assurance level 2 set forth in NIST Special Publication 800-63. [ii]

e) Feedback of the authentication information during the authentication process shall be obscured to protect the Data from possible exploitation/use by unauthorized individuals.

f) All Authorized Users shall communicate and authenticate credentials prior to access to Jersey Health Connect. Before any Data Exchange or Access, the Participant shall ensure its Authorized Users' credentials are in "good standing".

g) The Authorized User attempting to access the Patient Data shall be verified as having a Role type that is permitted to access the type of Data being requested from or through Jersey Health Connect.

h) Each request for Patient Data shall include a non-repudiable assertion as to the identity and role of the Authorized User who will receive the Data.

i) Each HIE connected to Jersey Health Connect shall maintain procedures that govern Authorized Users' ability to access information in or through the Connected HIE Participant's system and through Jersey Health Connect.

j) Appropriate sanctions against Authorized Users who fail to comply with this HIE Policies should be applied, including and up to termination of such Authorized User's access to Jersey Health Connect in accordance with JHC Policy 20, "Enforcement and Sanctions".[iii] Participants are responsible for maintaining Sanction Logs, which shall be provided to Jersey Health Connect upon request.

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 3.2, "Authentication." This policy and procedures requires verification that an individual authorized to access an NJHIO is who he or she claims to be and sets forth specific authentication requirements with a minimum of Level 2 authentication as set forth in NIST SP 800-63.

[ii] NJHIN Security Policy and Procedure 3.2 requires a minimum of Level 3 authentication as set forth in NIST SP 800-63 for **Remote VPN Access.**

[iii] See NJHIN Security Policy and Procedure 3.3, "Access," requiring termination and other sanctions for policy and procedural violations.