JERSEY Health Connect
Connecting your healthcare needs

HEALTH INFORMATION EXCHANGE POLICIES

Policy: Data Integrity and Correction Number: 18

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

Policy:

Jersey Health Connect shall protect the quality of care received by Patients, as well as the quality and accuracy of medical decisions and health care outcomes by creating an efficient, consistent and accurate system for moving Data throughout Jersey Health Connect.

Procedure:

1) Participants and Authorized Users must take reasonable steps to ensure that Data exchanged throughout Jersey Health Connect is accurate, complete, and up-to-date to the extent reasonably necessary for such Participant or Authorized Users intended purposes, and has not been altered or destroyed in an unauthorized manner.

2) Participants and Authorized Users are required to update or correct Data which they reasonably believe to be incorrect, incomplete or outdated. In the event such Data is corrected or updated, Participants and Authorized Users must timely notify other Participants and/or Authorized Users reasonably believed to have accessed or relied upon the information. To facilitate this process, each Participant's EMR must have the technical capability to "automatically" send updates and corrections to Jersey Health Connect, or, at a minimum, allow the Participant to "manually release" or "Push" updates and corrections of Data to Jersey Health Connect.

3) In the event a Participant must update or correct Data which has been provided to a Patient's PHR, whether requested by the Patient or otherwise, the Participant shall provide reasonable and timely notice of such changes to the PHR Vendor and the Patient.

4) Participants and Authorized Users must develop and monitor internal processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, PHI/Data.

5) Participants and Authorized Users shall implement **technical security measures** to protect against unauthorized access of Data that is being transmitted over an electronic communications network, in accordance with relevant provisions under the HIPAA Security Rule.

6) Participants and Jersey Health Connect shall implement methods for encryption and decryption, where appropriate, to protect Data stored and transmitted through Jersey Health Connect. Encryption strength of 128 bit or better shall be required. All portable media (e.g., mobile devices) shall not be used to store or transmit Data through Jersey Health Connect without approval from Jersey Health Connect and reasonable and appropriate encryption processes for such portable media.[i]
7) Jersey Health Connect shall implement security measures to safeguard electronically transmitted Data from undetected improper modification until properly disposed of. This includes implementation of electronic mechanisms to corroborate that Data has not been altered or destroyed in an unauthorized manner. [ii]

8) Jersey Health Connect shall develop processes to detect, prevent, monitor and mitigate any unauthorized changes to, or deletions of, Data.[iii]

9) The PHR Vendor shall comply with the requirements of this Policy and additionally implement security measures to safeguard Data transmitted from Jersey Health Connect and/or the Participants to the Patient PHRs.

10) The PHR Vendor shall inform Jersey Health Connect and/or the Participants of any Data it becomes aware of, or the Patient makes it aware of, which is incomplete, inaccurate or otherwise altered by an unauthorized individual. The PHR Vendor shall implement such administrative, technical and physical security measures as may be reasonable and necessary to prevent unauthorized access, changes or deletions of Patient Data maintained within PHRs. The PHR system should prevent accidental "deletion" of Data entered by Patients and prohibit deletion by Patients of any Data released into the PHR by Participants without affirmative action by the PHR Vendor. The PHR Vendor shall ensure that all employees and workforce members are appropriately trained in such security measures as well as all applicable JHC Policies and Procedures.

11) The PHR Vendor shall make all policies and procedures governing the PHR system clear and transparent to Patients, including, but not limited to, access to and self-entry of Data in the PHR, sources from which Data may come from, limited uses and disclosures it may make of Data, Data retention times, and expungement and Data transfer processes from the PHR. Any changes in such policies and procedures shall be promptly made available to Patients. The PHR Vendor shall be responsible for implementing policies and procedures as reasonable and necessary for Patients to amend Data they have self-entered into their PHR and to request amendments to Data released into the PHR by Participant(s).

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 3.6, "Encryption" **requires encryption** and/or **alternative security** for PHI in transit and at rest. Also NJHIN 5.0 "Minimum Security Standards" mandates specific security measures for Member computers and portable devices – a Member being an entity in a Participation Agreement with NJHIN.

[ii] NJHIN Security Policy and Procedure 3.7, "Data Retention and Destruction" requires NJHIOs to protect PHI from loss, destruction and falsification through appropriate security controls. See also NJHIN 5.0.

[iii] NJHIN Security Policy and Procedure 3.7. See also NJHIN 5.0.