

HEALTH INFORMATION EXCHANGE POLICIES

Policy: Auditing

Number: 17

Applicability: Viewer, Provider, Exchanger

Effective: 9/23/2013

Policy:

Jersey Health Connect maintains formal audit and accountability process for recording and examining access to, uses and disclosures of information in Jersey Health Connect as well as to verify compliance with access and authorization controls, administrative and other safeguards designed to prevent and/or limit unauthorized access to Data. This Auditing Policy also sets forth minimum requirements Participants must follow in tracking Authorized User log-ins, access to, and other activities relating to Data within Jersey Health Connect.

Procedure:

1) Participant Audit Logs

- a) Each Participant is required to maintain electronic Audit Logs, if possible, that document each time Data is accessed through Jersey Health Connect by a Participant, including its Authorized Users. This shall include any failed attempts such as invalid passwords or IDs.
- b) Participant Audit Logs shall include such information as may be necessary for a Participant to respond to an AOD as well as to detect any unauthorized uses, disclosures or modifications to Data. At a minimum, such Audit Logs shall include the following information:
 - i) Identity of the Patient whose PHI/Data was accessed;
 - ii) Identity of the Authorized User accessing the PHI/Data and the identity of the Participant with which he/she is affiliated;
 - iii) Type of PHI/Data or other record accessed (e.g., pharmacy data, clinical laboratory data) with 'sensitive data' specifically identified;
 - iv) Date and time of the access;
 - v) Source of the PHI/Data (the Participant from whose records the accessed PHI/Data was derived or maintained by); and
 - vi) Unsuccessful log-in attempts.
 - vii) Audit Logs must be immutable, i.e., the log information cannot be capable of being altered by anyone regardless of access privileges, or that any alterations are conspicuously made evidence.

viii) Any irregularities such as alterations or unauthorized log-ins or log-in attempts shall be documented and appropriate mitigating action taken by the Participant.

ix) Participant Audit Logs shall be maintained for a period of at least six (6) years from the date on which PHI/Data is accessed.

2) Jersey Health Connect Audit Logs

a) Jersey Health Connect must maintain Audit Logs to track all activities involving electronic PHI. System requirements for maintaining such Logs shall include software applications, firewalls, servers, and other appropriate hardware and/or software as may be needed to facilitate the maintenance of such Logs.ⁱ

b) Jersey Health Connect Audit Logs shall include, at a minimum, the following information:ⁱⁱ

i) Identity of the Patient whose PHI/Data was accessed;

ii) Identity of the Authorized User accessing the PHI/Data and the identity of the Participant with which he/she is affiliated;

iii) Type of PHI/Data or other record accessed (e.g., pharmacy data, clinical laboratory data) with 'sensitive data' specifically identified;

iv) Date and time of the access;

v) Source of the PHI/Data (the Participant from whose records the accessed PHI/Data was derived or maintained by);

vi) All messages between Participants and/or Authorized Users that pass through Jersey Health Connect for a set period of time; and

vii) Unsuccessful log-in attempts.

3) Periodic Auditingⁱⁱⁱ

a) Jersey Health Connect and Participants must ensure that annual and periodic auditing is performed to monitor compliance with all relevant HIE policies and internal policies as well as all applicable laws, rules and regulations.

b) Jersey Health Connect may conduct random periodic audits on a sample of Participants. Participants shall cooperate by producing documentation supporting the audit as may be requested by Jersey Health Connect.

c) At a minimum, Jersey Health Connect and Participants shall audit or direct a third party to audit;

d) Required documentation for Patients whose PHI/Data is maintained and accessed by the Participant; and

e) With the exception of "Break Glass" functions, that Authorized Users who access PHI/Data through Jersey Health Connect are Authorized to access the

PHI/Data for a Permitted Purpose in accordance with the JHC Permitted and Prohibited Uses Policy and all other applicable laws, rules and regulations; and

f) For “Break Glass” functions, that applicable requirements are met when PHI/Data was accessed through such function, or as may be appropriate through the JHC Information Afforded Special Protection Policy.

g) Audits shall be conducted at a minimum on a bi-annual basis. Participants shall consider their own risk analyses and organizational factors, such as current technical infrastructure, hardware and software security capabilities, in order to determine a reasonable and appropriate frequency with which to conduct audits more often than annually.

4) Access to Participant Audit Logs ^{iv}

a) Participants shall provide Jersey Health Connect or a requesting Participant, with the following information regarding any Patient whose PHI/Data was accessed through Jersey Health Connect:

b) The name of each Authorized User who accessed such Patient’s PHI/Data in the prior 6-year period;

c) The time and date of such access; and

d) The type of PHI/Data or record that was accessed (e.g., clinical data, laboratory data, etc.).

e) Participants shall provide such information to Jersey Health Connect or a requesting Participant as promptly as is reasonably practicable, but no later than ten (10) calendar days after receipt of the request.

f) Audit Logs are not part of a Designated Record Set. Therefore, Patients do not have automatic rights to access a Participant’s Audit Log, except to the extent such information may be required to respond to an Accounting of Disclosures or other HIPAA or HITECH obligation.

g) Jersey Health Connect may facilitate the gathering and production of such Audit Logs to allow Participants to comply with their obligations under HIPAA and HITECH.

5) PHR System Auditing

a) PHR Vendor Audit Logs and Audit Mechanisms.

b) The PHR Vendor shall be responsible for maintaining Audit Logs that document and track each time Data is used and disclosed within a Patient’s PHR and all other activities related to the Patient’s PHR. Such Audit Logs shall be immutable and otherwise in compliance with this Policy. The PHR Vendor shall be responsible for ensuring that PHR audit controls, logs and other mechanisms are in place to identify Data entered into the PHR by the Patient and Data

entered into the PHR by the Jersey Health Connect and/or Participants as well as the date and time of each entry.

c) Such Audit Logs and mechanisms shall additionally be in compliance with industry standards and include at a minimum:

d) All PHR account activity, including log-in attempts and failures, length of sessions and log-out events, of Patients and their authorized representatives.

e) Transactions by Participants (e.g., Data “pushed” into PHR), Patients, Proxy accounts and the PHR Vendor, including creation and modification of Data, “viewing”, “exporting”, “importing”, “printing”, “deletion” and dispute indications, where supported by the PHR Vendor.

f) Record of consents, authorizations and revocation forms (e.g., that may be scanned and uploaded into the PHR for Patient access)

g) The PHR Vendor shall be responsible for maintaining such Audit Logs for a minimum of six (6) years or such longer time period as is reasonably necessary and appropriate in accordance with commercial guidelines and best practices, or as may be required by law. Such Audit Logs or reports shall be made available to Jersey Health Connect promptly upon its reasonable request for such logs or reports.

h) The PHR Vendor shall implement other audit mechanisms as reasonably necessary and appropriate to ensure compliance with all applicable JHC Policies and Procedures, as well as state and federal law. This shall include, at a minimum, software applications, firewalls, services and other appropriate system requirements in accordance with commercial guidelines and best practices, or as may be required by law.

i) The PHR Vendor shall perform periodic auditing and reports to monitor system and workforce compliance with all applicable JHC Policies and Procedures, as well as state and federal law, and document the results of such auditing. The PHR Vendor shall provide Jersey Health Connect with summaries of such reports promptly upon the reasonable request of Jersey Health Connect.

j) The PHR Vendor shall ensure that Patients have access to the same information maintained within the Audit Log within the respective PHRs so that Patients may be made aware of all significant activities and transactions pertaining to Data maintained within their PHRs. This shall include at a minimum, the identify of the individual accessing the PHR or releasing information into the PHR, the date, time and source of the information being accessed, and clear indication of any amendments that have been made to the PHR.

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 3.4, “Audit” requires NJHIOs to maintain Audit Logs **documenting all access of PHI via the NJHIN** and **strongly recommends each NJHIO separate duties** between those who administer access control functions and those who administer audit trails. Audit logs must be maintained for a period of at least **six (6) years** from the date information was accessed.

ⁱⁱ NJHIN Security Policy and Procedure 3.4 also requires the audit log include at a minimum specific information, including (i) dates and time of event; (ii) patient identification; (iii) user identification; (iv) access device or origin of the request and type of action; (v) identification of the data accessed (optional); and (vi) capture of system startup and shutdown functions.

ⁱⁱⁱ NJHIN Security Policy and Procedure 3.4 also sets forth NJHIO obligations to conduct periodic audits, at least once annually, in auditing the activities of all or a statistically significant subset of the NJHIO’s Members (JHC Participants).

^{iv} NJHIN Security Policy and Procedure 3.4 also requires NJHIOs to make available to their **Members/Participants** upon request certain information from their audit logs concerning a patient of such Member/Participant whose PHI was accessed through the NJHIN, as well as access to audit information **by Patients AND to the public**. See also JHC Policy 4, “Patient Rights” for accounting of disclosure obligations.