

BARNABAS HEALTH

POLICY # HIE-14

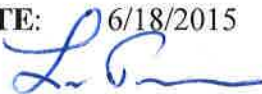
INFORMATION TECHNOLOGY AND SERVICES

POLICY

TITLE: Auditing

EFFECTIVE DATE: 6/18/2015

APPROVED BY:



System:

System Chief Information Officer/
Barnabas Health

Date:

8/6/2015

ATTACHMENTS:

None

PURPOSE:

To ensure that routine and random audits are utilized as useful oversight tools for recording and examining access to information through the BHIE (e.g., who accessed what data and when), and to verify compliance with access controls and administrative and other safeguards developed and implemented to prevent/limit inappropriate access to Data. This policy also sets forth minimum requirement that Participants shall follow in connection with tracking their Authorized Users log-on and access to Data through the BHIE.

POLICIES:

1. Maintenance of Audit Logs

- a. Each Participant is required to maintain audit logs that document all access of Data/PHI through the BHIE by a Participant, including its Authorized Users, ("Audit Logs") as follows:
 - i. The Participant is responsible for maintaining and generating any audits reflecting queries, access and disclosures taking place within the Participants' own EMR;

- ii. The BHIE will maintain and generate any audits reports reflecting queries, access and disclosures that take place through the BHIE.
 - b. Audit Logs shall, at a minimum, include the following information:
 - i. The identity of the Patient whose PHI/Data was accessed;
 - ii. The identity of the Authorized User accessing the PHI/Data;
 - iii. The identity of the Authorized User and with which Participant he/she is affiliated;
 - iv. The type of PHI/Data or record accessed (e.g., pharmacy data, laboratory data, etc.);
 - v. The date and time of access;
 - vi. The source of the PHI/Data (i.e., the identity of the Participant from whose records the accessed PHI/Data was derived); and
 - vii. Unsuccessful access (log-in) attempts.
 - c. Audit Logs shall be immutable. An immutable Audit Log requires either that log information cannot be altered by anyone regardless of access privilege or that any alterations are tamper evident.
 - d. Audit Logs shall be maintained by the BHIE Program Manager for a period of at least six (6) years from the date on which information is accessed.

2. Obligation to Conduct Periodic Audits.

- a. Each Participant will ensure that periodic audits are performed to monitor use of the BHIE by its respective Authorized Users and applicable employees and staff in order to ensure compliance with the policies and procedures of such Participant, the BHIE and all applicable laws, rules and regulations.
- b. Periodic audits shall be conducted by Participants. Participant and Authorized Users shall consider their own risk analyses and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine the reasonable and appropriate frequency with which to conduct audits more often than annually.
- c. The BHIE will conduct periodic audits on a random sample of Participants. The scope of the audits will be designed in consultation with the Chief Medical Information Officers, the local Chief Medical Officers, Internal Audit, the BHIE Program Manager, BHIE Privacy Officer, and BHIE Security Officer. Participants shall cooperate with producing documentation supporting auditing as requested by the BHIE.

- d. The BHIE may perform, and each Participant and Authorized User agreed to submit to, additional reasonable investigation based upon an audit report suggesting potential improper or impermissible access or use of the BHIE.

3. Access to Audit Logs.

- a. Each Participant shall provide the BHIE, or the requesting Participant, upon request, with the following information regarding any Patient whose Data was accessed through the BHIE:
 - i. The name of each Authorized User who accessed such Patient's PHI/Data in the prior 6-year period;
 - ii. The time and date of such access; and
 - iii. The type of PHI/Data or record that was accessed (e.g., clinical data, laboratory data, etc.).
- b. All Participant and Authorized User shall only be entitled to receive Audit Log containing PHI if such disclosure of PHI is permitted under HIPAA, or if a written authorization was obtained from the Patient whose PHI is being disclosed, or the information is otherwise de-identified.
- c. Participant shall provide such information as promptly as reasonably practicable but in no event more than 10 calendar days after receipt of the request

4. Patient Access to Audit Information

- a. Audit Logs are not to be considered part of a Designated Record Set, and patients do not have automatic right to access such logs. Such audit logs may, however, be used, including components thereof, to respond to a patient's request for an Accounting of Disclosures, if required by law.
- b. The BHIE may facilitate the gathering and producing of such logs to allow Participant to comply with its obligations under HIPAA.

QUALIFICATIONS: NA

EQUIPMENT: NA

PROCEDURE:

DOCUMENTATION: NA

INFECTION CONTROL: NA

SAFETY: NA

SECURITY OVERSIGHT GROUP (SOG) Approve for Release:

REFERENCES:

ORIGINAL DATE: 6/18/2015

REVIEWED DATE(S):

REVISED DATE(S):