Kansas Department of Health and Environment
POLICIES AND PROCEDURES

P&P 07: Audits

Date Approved: 11/09/2011
Date Reviewed: 03/01/2017
Date Updated: 05/09/2017

Purpose:

To establish procedures to monitor usage to prevent and identify unauthorized access to PHI.

Policy:

1) An approved HIO shall have the capability to generate complete and accurate audit logs going back a period of at least three (3) years to identify the following:
   a) each User (including approved HIO staff) who accessed an individual's PHI through the HIO during a specified period of time when such information is readily available (including the time, date, the type of PHI accessed, and the Participant with which the User was associated at the time (if applicable));
   b) those patients for whom a User accessed PHI through the HIO during a specified period of time (with the same level of detail);
   c) any occasion on which PHI for which an individual requested restrictions (see P&P 02, Patient Notice and Restrictions on Access) was accessed (with the same level of detail);
   d) all log-in attempts during a specified period of time and/or for a particular Participant or User; and
   e) any and all User IDs assigned to a specific individual when such information is readily available.
2) An approved HIO shall employ immutable audit logs or otherwise ensure that such logs cannot be altered. Any audit log produced by the HIO to a third party in electronic format shall be in read-only format.
3) An approved HIO shall establish, maintain, and document a process by which, at a minimum:
   a) an approved HIO shall deliver to a Participant (including a former Participant) within thirty (30) days of receipt of a written request an audit log described in Section 1(a) regarding the requesting Participant's current and/or former Users; and
   b) an approved HIO shall deliver to an individual (or the individual's personal representative) within thirty (30) days of receipt of a written request an audit log described in Section 1(b)

regarding the individual. An HIO shall not charge for responding to an individual's first request during a calendar year, but may impose a reasonable fee for responding to additional requests during a calendar year, unless the request is based on a reasonable suspicion of an unauthorized disclosure of the individual's PHI.

c) An approved HIO shall establish, maintain, and document an internal audit plan to monitor Participants' compliance with the Participation Agreement through review and analysis of audit logs for a statistically significant sample of Users.

   i) The HIO shall determine, based on its risk analysis and organizational factors (e.g., technical infrastructure, hardware and software security capabilities) the appropriate frequency for such audits. At a minimum, such audits shall be conducted (a) as part of the HIO's response to any suspected or confirmed security breach; and (b) on an annual basis.

   ii) Within a reasonable period of time following completion of the audit, the HIO shall develop and implement a corrective action plan to address any anomaly noted in the report. Such corrective action plan shall include appropriate punitive and/or remedial actions to be taken against any Participant or User involved in unauthorized access to PHI.

   iii) The HIO shall produce to KDHE upon request any audit log, audit report, or corrective action plan.

4) An approved HIO shall require in its Participation Agreement that a Participant shall:

   a) cooperate fully with any inquiry from or investigation by the HIO or KDHE regarding unauthorized access to PHI;

   b) promptly report to the HIO any unauthorized access to PHI through the HIO of which the Participant becomes aware as soon as possible, but not to exceed three (3) business days of its discovery; and

   c) take appropriate action in response to any unauthorized access to mitigate any harm and prevent similar occurrences in the future. As necessary, the approved HIO shall assist the Participant in the investigation of any reported unauthorized access and/or the development and implementation of an appropriate corrective action plan in response to such unauthorized access.