Kansas Department of Health and Environment
POLICIES AND PROCEDURES

P&P 06: Authentication

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

Purpose:

To identify the requirements to which an approved HIO must adhere with respect to authentication of a User to access PHI through the HIO.

Policy:

1) An approved HIO shall maintain a written policy consistent with this P&P 06 regarding the requirements and procedures for User authentication necessary for a User to access an individual's PHI through the HIO on a specific occasion. An HIO shall require in its Participation Agreement that a Participant comply with such requirements and procedures.
2) KDHE shall review HIO User authentication policies during the HIO application process and may audit approved HIOs for compliance with this P&P 06.
3) An approved HIO shall comply with the HIPAA Security Rule Administrative Safeguards for Log-In Monitoring and Password Management and shall require in the Participation Agreement that its Participants comply with such Administrative Safeguards when accessing PHI through the HIO.
4) An approved HIO shall establish and enforce standards for User passwords including, but not limited to, password strength requirements (based on the then-current version of NIST SP 800-63 (or successor publication)); re-setting and re-use of passwords; and response to failed access attempts. Password standards shall apply equally to Participants with "single sign-on" for electronic health record (EHR) and HIO access.
5) An approved HIO shall enforce an automatic log-off after a period of inactivity. Such termination shall remain in effect until the User re-establishes access to the HIO through authentication procedures. An HIO shall establish the length of periods of inactivity that will trigger such termination based on internal risk analysis and current technical infrastructure.