

Kansas Department of Health and Environment POLICIES AND PROCEDURES

P&P 09: HIO Minimum Approval Standards

Date Approved: 10/02/2012
Date Reviewed: 03/01/2017
Date Updated: 05/09/2017

Purpose:

To specify the minimum requirements an HIO must satisfy to be eligible for a Certificate of Authority. Unless otherwise specified, a reference to "Certificate of Authority" herein includes a Temporary Certificate of Authority.

Policy:

KDHE has established minimum approval standards relating to an HIO's business operations for three purposes:

- 1) properly safeguarding the privacy and security of protected health information exchanged by the approved HIO's Participants from any unauthorized disclosure;
- 2) achieving KDHE's goal of statewide health information exchange; and
- 3) ensuring the sustainability of approved HIOs.

An HIO must demonstrate full compliance with each of these minimum approval standards to be eligible for a Certificate of Approval to operate an approved HIO in the State of Kansas (except KDHE may waive full compliance with a specific standard by an approved HIO for good cause shown by the HIO, provided such waiver is consistent with the purposes identified above). The procedures for determining an HIO's compliance with these standards are set forth in P&P 10, Approved HIO Certificate of Authority. An HIO's compliance with these standards does not entitle the HIO to receive a Certificate of Authority. An approved HIO must demonstrate ongoing compliance with each of these standards to maintain its Certificate of Authority.

Minimum Approval Standards:

- 1) Participation Agreement. An approved HIO shall permit only Eligible Entities that have signed and adhere to all terms of a Participation Agreement that conforms to all KDHE requirements to participate in health information exchange. See P&P 04, Conditions of Participation. A Participation Agreement shall incorporate a Qualified Service Organization Agreement as required under 42 C.F.R Part 2 and a Business Associate Agreement as required under the HIPAA Privacy Rule.
- 2) Any Willing Participant. An approved HIO shall not refuse to enter into a Participation Agreement with any Eligible Entity on any basis except the following: (a) the Eligible

Entity refuses to accept KDHE-mandated contractual terms; (b) the Eligible Entity demands contractual terms that are inconsistent with KDHE-mandated terms; (c) the Eligible Entity refuses or is unable to pay the rates established by the approved HIO; (d) the Eligible Entity (if a health care provider) does not utilize a certified EHR product (with the exception of an Eligible Entity that seeks access to a provider portal only); or (e) the Eligible Entity otherwise does not satisfy the requirements set forth in KDHE P&P 04, Conditions of Participation.

- 3) Reasonable Fees. An approved HIO shall not charge any Eligible Entity fees for connection to or participation in health information exchange through the approved HIO that are unreasonable, excessive, or unfairly discriminatory.
- 4) Business Plan. An approved HIO shall develop, maintain, and regularly update a business plan with respect to the HIO's operations in the State of Kansas including, but not limited to, the following: (a) plans to achieve financial sustainability; (b) plans to ensure necessary technical capacity to support all electronic capabilities for transmission of clinical transactions necessary for Participants to satisfy then-current requirements relating to health information exchange to achieve meaningful use of certified electronic health records; (c) plans to maintain compliance with then-current industry standard security practices; and (d) adoption and adherence to good governance practices. An HIO shall submit to KDHE its then-current business plan for operations in the State of Kansas with its application for a Certificate of Authority (see P&P 10 – Approved HIO Certificate of Authority) and approved HIO shall submit to KDHE any substantive revisions to such business plan in a timely manner.
- 5) Participant Monitoring. An approved HIO shall establish and maintain a program for regular monitoring of each Participant's compliance with those provisions of the Participation Agreement regarding the privacy and security of health information exchange to assure compliance with those requirements.
- 6) HIPAA Privacy and Security Rules. An approved HIO shall comply with applicable HIPAA Privacy and Security Rule requirements with respect to the HIO's operations in the State of Kansas including, but not limited to: (a) maintaining and adhering to required policies and procedures and related documents and forms; (b) appointing qualified Privacy and Security Officers vested with appropriate authority; (c) requiring each member of its governing body and workforce to (i) complete annual training regarding the HIO's HIPAA Privacy and Security Rule policies, and (ii) execute and adhere to an adequate confidentiality agreement; (d) requiring any third-party vendor with which it does business to comply with applicable HIPAA Privacy and Security Rule requirements and the HIO's HIPAA Privacy and Security Rule policies; and (e) promptly and thoroughly investigating any suspected violation of the HIO's HIPAA Privacy and Security Rule policies and taking appropriate remedial and proactive measures in response to any confirmed violation including, but not limited to, prompt notification to KDHE and any and all individuals and Participants impacted by the violation.
- 7) Interoperability and Meaningful Use. To the fullest extent possible given technical limitations, an approved HIO shall in good faith pursue interoperability with
 - a) all other approved HIOs operating in the State of Kansas;

- b) all ONC-certified electronic health record vendors operating in the State of Kansas;
 - c) KDHE-identified government agency databases. An approved HIO shall participate in activities related to design, develop, modify, and implement agency databases that will incorporate HIO-supplied data to databases including but not limited to Medicaid, public health registries and other government agency databases; and
 - d) HIOs operating in other states. An approved HIO shall provide its Participants with the technical means to satisfy then-current requirements relating to health information exchange to achieve meaningful use of certified electronic health records, subject to the capabilities of a Participant's certified electronic health record.
- 8) NwHIN and Direct. An approved HIO shall, directly or indirectly, meet requirements established for utilizing NwHIN and Direct and corresponding standards within the federally mandated timeline or within the timeline established by KDHE (if any).
- 9) Technical Capacity. With respect to the operations of health information exchange in the State of Kansas, an approved HIO shall have administrative and/or technical capacity to perform as follows:
- a) At a minimum, receive from Participants and Data Sources and make available through electronic health information exchange all categories of information included in the Minimum Data Set as specified in P&P 04, Conditions of Participation.
 - b) Reliably and accurately identify the source of data made available by Participants and Data Sources; track Participant inquiries by User, when readily available; and produce audit trails for all health information exchange activities.
 - c) Publish, provide, and monitor the provision of on-line, batch, and customer support services within formal services levels as documented in the approved HIO's Participation Agreements.
 - d) Monitor system capacity; maintain system availability; and develop and maintain appropriate business continuity and disaster recovery procedures.
 - e) Establish and maintain a reliable patient matching process with a specified degree of certainty.
 - f) Take action on individuals' requests for restrictions on access to their PHI and requests to lift such restrictions received from KDHE as soon as practicable.

An approved HIO shall arrange for regular and appropriate third-party technical audits and furnish such audit reports to KDHE upon request.

11)10) Financial Policy. An approved HIO shall use financial policies and procedures that conform to generally accepted accounting principles, shall have an independent audit of its financial statements performed on an annual basis, and shall have the resources and capabilities to continue to function as a going concern.

12)11) Corporate Compliance Program. An approved HIO shall conduct its business operations in conformance with all KDHE policies and procedures and applicable state and federal laws and regulations. An approved HIO shall develop and maintain an effective

corporate compliance program consistent with guidance issued by the Department of Health and Human Services Office of Inspector General.

~~13)~~12) **Reporting.** An approved HIO shall submit complete and accurate written quarterly reports regarding operations, future plans, and material changes to items 1 through 11 of P&P 9: HIO Minimum Approval Standards. Written reports may be submitted as PDF files emailed to KDHE.HealthStatistics@ks.gov.

Additional Standards for Approved HIOs Operating Under Temporary Certificates of Authority

- 1) An approved HIO shall cooperate with the other approved HIO and shall devote adequate resources to achieve interoperability between the two approved HIOs within a reasonable period of time not to exceed June 30, 2013.
- 2) An approved HIO shall cooperate with the other approved HIO to establish in a timely manner secure and reliable interfaces with Health Information Organizations operating in adjacent states, the NWHIN, and appropriate data sources including, but not limited to, KDHE Web-IZ, KDHE Trisano, CDC BioSense, and centralized repositories of diagnostic test results and filled pharmaceutical prescriptions.
- 3) Beginning on July 1, 2012, an approved HIO shall submit monthly progress reports to KDHE regarding implementation of such interoperability and interfaces.