Kansas Health Information Network, Inc. d/b/a KONZA National Network

HIE Policy and Procedures Policies

The Kansas Health Information Network, Inc. (KHIN) d/b/a KONZA National Network (KONZA) policies and procedures apply to all of the organizations that KHIN does business as (d/b/a) in other states. In 2024 this includes KHIN (Kansas), Carolina eHealth Network (South Carolina), CTHealthLink (Connecticut), HealtheParadigm (Georgia), HealthSYNC (Louisiana), GenesisLink (Texas), OneHealth New Jersey (New Jersey), SHINE (Missouri), MHAX (Mississippi), and KONZA HIE.

KONZA Policies and Procedures Summary

Policy Number and Title	Subject	Summary
Policy #001 Coordination Policy	Compliance with laws, policies, and procedures	Requires participants to comply with all laws, KONZA's policies and procedures, and establish their own internal, compliance procedures.
Policy #002 Policies and Procedures	KONZA Policies and Procedures	Confirms KONZA's obligation to adopt, maintain, and administer KONZA policies and procedures and confirms participants' obligation to follow such policies and procedures.
Policy #003 Participant Policy	Participation Requirements	The purpose of this policy is to outline requirements to participate in the KONZA Designated Network, the policies for onboarding new participants, and to state preconditions for availability and use of a new Participant's data.
Policy #004 Participant Privacy and Security Policy	Participant Privacy and Security Policies and Procedures/Notice to Patients/Consent/Opt-Out	Reiterates participants' obligations regarding privacy and security policies/procedures; describes best practices for notifying patient of participants' use of KONZA; confirms KONZA's requirement that patients sign a consent regarding use/disclosure of patient data through KONZA to the extent required by law; identifies the website for patients to use to restrict the use of their data through the KONZA; addresses certain other privacy and security practices.
Policy #005 Data Use, Reporting, and Analytics Policy	Data Use	Defines the policy and procedures regarding authorized use and disclosure of participants' data in connection with KONZA.
Policy #006 Security Override for Point-of Care Disclosure to Participants	Restrictions on use/disclosure of Part II PHI and Sensitive Information/Override for Emergencies and Patient Authorized Point of Care Disclosure	Identifies restrictions on use/disclosure of Part II PHI and on the use of PHI restricted by the patient; outlines the process for security override at the request (and with the consent) of the patient for a specific instance of care; describes the process for security override in the event of an emergency.
Policy #007 Restrictions of Use of Sensitive Information	Restrictions on Use of Sensitive Information	Prohibits disclosure of Protected Health Information that requires patient authorization prior to disclosure unless participant obtains proper, written authorization from patient.

Policy Number and Title	Subject	Summary
Policy #008 Policy Governing Data for Patients who Self-Pay for Healthcare	Policy Governing Data for Patients who Self-Pay for Healthcare	Defines the responsibilities and handling of self-pay healthcare data.
Policy #009 Information Blocking Policy	Policy on Information Blocking	Policy defining responsibility to respond and share ePHI, along with exceptions for not responding to requests for data sharing.
Policy #010 Policy Dispute Management and Participant Enforcement	Policy Dispute Management and Participant Enforcement	Defines the handling of disputes in KONZA Designated Network and the process for participant enforcement
Policy #011 Data Breach Response Policy	Steps for reporting, investigating, and resolving suspected security incidents.	Outlines the management of any suspected security incidents
Policy #012 Mitigation Policy	Mitigation in the event of unauthorized use	Requires Participants and KONZA to mitigate with appropriate remedial action in the event an unauthorized use or disclosure occurs.
Policy #013 Auditing and Reporting Policy	Audit Controls/Time Frames for Reporting Unauthorized Use/Disclosure	Describes the process KONZA uses in conjunction with Participants to audit use and disclosure through KONZA to confirm participants' proper use/disclosure of data through KONZA; establishes time frames within which participants must notify KONZA in the event of participants' unauthorized use of KONZA data.
Policy #014 Technical Framework Policy	Technical Framework Policy	Defines the administrative oversight and governance provided by the Designated Network Governance Body and Technology Vendor Review Committee for the KONZA Designated Network.
Policy #015 Security Password Policy for Participants	KONZA Password Requirements	Identifies the password requirements participants must implement for their authorized users prior to allowing them to use KONZA.
Policy #016 User Access	Access and Removal of Access	Identifies the process for granting participants a right to access KONZA; identifies the process for revoking participants' access rights to KONZA.

Coordination Policy	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 001
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

A. Laws. KONZA and each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. KONZA and each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure compliance.

B. Policies and Procedures. Each Participant shall, at all times, comply with all applicable Policies and Procedures. These Policies and Procedures may be revised and updated periodically. Each Participant will receive written notification of revisions and updates consistent with the requirements of the applicable Data Sharing Participation Agreement. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Policies and Procedures applicable to it.

C. Participant Policies and Procedures Each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and the applicable KONZA Policies and Procedures.

Policies and Procedures	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 002
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE
KONZA Policies and Procedures describe in detail the governance and operational functions of the KONZA Designated Network. The implementation of the KONZA Policies and Procedures is essential for effective operation of the KONZA Designated Network.

POLICY
1. Every Participant prior to making use of the KONZA Designated Network has agreed in the Participation Agreement to abide by the KONZA Policies and Procedures.

2. Except where otherwise specified in an individual Policy, the KONZA Policies and Procedures apply to all Participants and their respective Authorized Users, as well as to KONZA, support staff members hired by KONZA or hired by or affiliated with Participants, Board members, Committee members, information technology staff designee(s), and other agents of Participants who receive access to KONZA, or health information submitted to, maintained on, or retrieved from KONZA.

3. To comply with the conditions of the Participation Agreement, KONZA has established, and will periodically modify, certain KONZA Policies and Procedures. Compliance with the Policies and Procedures is a requirement for all Participants.

4. Change Management
    a. KONZA Policies and Procedures are reviewed annually.
    b. The Designated Network Governance Body (DNGB) approves all changes to the KONZA Policies and Procedures
    c. Each Participant will have the right to request reconsideration of a change to the Policies and Procedures and/or terminate its Participation Agreement in the event it is unable to comply. KONZA retains the sole right to either grant or deny the request.
        i. Such requests will be presented to the DNGB for final approval.

WHO IS AFFECTED
Except where otherwise specified in an individual Policy, the KONZA Policies and Procedures apply to all Participants and their respective Authorized Users, as well as to KONZA, support staff members hired by KONZA or hired by or affiliated with Participants, Board members, Committee members, information technology staff designee(s), and other agents of Participants who receive access to KONZA, or health information submitted to, maintained on, or retrieved from KONZA.

RESPONSIBILITY
KONZA is responsible for the development, implementation, maintenance, and administration of the KONZA Policies and Procedures. KONZA will approve policies and from time to time may amend, revoke, or add to existing policies.

POLICY REVIEW CYCLE
The KONZA Policies and Procedures must be reviewed on an annual basis by KONZA. All versions of the individual Policies and Procedures shall be retained for 7 years.

Participant Policy	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 003
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE

The purpose of this policy is to outline requirements to participate in the KONZA Designated Network, the policies for onboarding new participants, and to state preconditions for availability and use of a new Participant's data.

POLICY

1. Participants are evaluated to ensure they have the necessary legal, technical, and operational capabilities to meet the requirements of the KONZA Designated Network.

2. It is the Participant's responsibility to maintain the quality of its records that will be available in the KONZA Designated Network.

PROCEDURE

The following conditions must be met before a new Participant's data is made available to KONZA for use in clinical decision making:

1. The Participant will have met notification requirements consistent with the KONZA Privacy and Security Policy.

2. Each Participant shall actively participate in a process by which its data will be reviewed and approved. Within 10 days of completion of this process, the Participant must sign a User Acceptance Testing (UAT) form. If the form is not signed KONZA will confirm the accuracy of the data and make it available upon confirmation.

3. Each Participant shall have implemented and maintained an ongoing Data Quality Plan pertaining to data the Participant provides to KONZA.

4. KONZA will move Participants into production upon receipt of the signed UAT form or after 10 business days with confirmation of data accuracy.

Participant Privacy and Security Policy	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 004
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE

The purpose of this policy is to outline participants' obligations regarding privacy and security policies/procedures; describe best practices for notifying patient of participants' use of Kansas Health Information Network, Inc. (HIO); confirm HIO's requirement that patients sign a consent regarding use/disclosure of patient data through HIO to the extent required by law; identify the website for patients to use to restrict the use of their data through the HIO; address certain other privacy and security practices.

POLICY

A. General Requirements

1. Each Participant must have established internal privacy and security policies and procedures that effectively manage access to, and the appropriate use of, Protected Health Information (PHI). Each Participant must confirm that its internal policies comply or are updated to comply and meet all requirements established by HIO and any applicable laws. Except as otherwise allowed by the Participation Agreement or HIO's policies and procedures, Participants shall obtain prior written approval from the HIO before permitting a business associate (other than Authorized Users of the HIO itself), to access HIO or to obtain data from HIO.

2. HIO is committed to the responsible and appropriate use of PHI submitted to, maintained on, and accessed from HIO for the permitted uses identified in the Data Sharing Participation Agreement. HIO shall:
   (a) Provide supporting information, rules, and standards for Participants;
   (b) Foster compliance with appropriate use of PHI by Participants for the care and/or care coordination of individual patients while respecting the patient's right to privacy;
   (c) Protect PHI from unauthorized use by the contributing Participants by establishing mechanisms for authorizing, granting, removing, and reporting user access thereto; and
   (d) Utilize commonly accepted security practices for the protection of the information entrusted to it.

B. Sensitive Protected Health Information/Notice to Patients Regarding HIO

HIO will facilitate certain rights provided by Participants to their patients whose information is shared through HIO. In certain situations regarding certain types of Protected Health Information, federal and state law may impose more restrictive privacy rules to such sensitive Protective Health Information (Sensitive Health Information) than HIPAA. Depending upon the purposes for which Sensitive Health Information is being sought, the law may require a patient to specifically authorize in writing the disclosure of Sensitive Health Information by signing an authorization for disclosure that contains certain elements. Sensitive Health Information may include but is not limited to:

- Substance abuse records
- Mental health and psychotherapy records
- Genetic testing information
- HIV/AIDS information

- Developmental disability records
- Communicable disease information

Participants shall not disclose through the HIO Sensitive Health Information that requires the execution of a specific, written authorization unless Participant has obtained any required authorization for disclosure from the patient prior to disclosing the Sensitive Health Information through the HIO. Responsibility for restricting the transmission of Sensitive Health Information will reside with the Participant. The transmitting Participant shall obtain an appropriate authorization from the patient in accordance with applicable law prior to disclosing or re-disclosing Sensitive Health Information through the HIO.

Participants will add explanatory text regarding HIO to their online and hard copy versions of their Notice of Privacy Practices (NPP) 30 days prior to going "live" with the HIO. The additional language to be added to the Notice of Privacy Practices can be found on HIO website. HIO will provide a brochure that Participants can make available to patients. The brochure will explain the purpose of the HIO.

C. Restriction of PHI Requirements and Procedures

Patients can find direction on how to restrict the use and disclosure of their PHI through the HIO website.

A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her accessible through HIO. If an individual requests that his/her PHI not be shared through HIO, the PHI will not be accessible to other Participants in HIO without the patient's written consent or in the event of a medical emergency.

D. Communications Between HIO and Participants

All electronic communications between HIO Participants and HIO containing protected health information (PHI) will be done using HIO's secure clinical messaging. If this preferred method of electronic communication is not available to a Participant, then the Participant will use a HIO approved method that utilizes an encryption/decryption method and a means to authenticate the communicating parties and the message.

E. Uses and Disclosures of PHI

1. Compliance with Law. All disclosures of PHI through the HIO and the use of such information obtained from Participants and HIO shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing PHI for a particular purpose, the requesting Participant shall obtain the required documentation or meet the requisite conditions and shall provide evidence of such at the request of the disclosing institution.

2. Purposes. A Participant may provide or request PHI through HIO only for purposes permitted by the applicable Participation Agreement, subject to any applicable law or regulation. Participants may access their own vault for support and maintenance purposes. Information may not be requested for marketing or marketing related purposes. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request information through HIO.

3. HIO and Participant Policies. Uses and disclosures of and requests for PHI via HIO shall comply with all HIO Policies and Procedures. In addition each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of PHI and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.

4. Audit Logs. As provided in HIO Auditing and Reporting Policy, Participants and HIO shall work together to maintain an audit log documenting which Participants posted and accessed the information about an

individual through HIO and when such information was posted and accessed. See policy on Auditing and Reporting.

5. Authentication. HIO shall issue to Participants unique user IDs and HIPAA compliant passwords for the Participants distribution to their Authorized Users. In addition, each Participant shall have and follow its own internal security requirements for verification and authentication of those Authorized Users within its organization who shall have access to information through HIO's shared data system.

G. Amendment of Data

Each Participant shall comply with applicable federal, state, and local laws and regulations regarding individual rights to request amendment of PHI. If an individual requests, and the Participant accepts an amendment to the PHI about the individual, the Participant will submit updates to HIO. If requested by the Participant, HIO shall assist the Participant in notifying other relevant Participants of any amendments.

Data Use, Reporting and Analytics Policy	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 005
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE:
The purpose of this Policy is to establish a framework and guidelines pursuant to which KONZA may perform Data Aggregation, Data Reporting and Analytics for Treatment, Payment, Health Care Operations, Public Health, Research, and other purposes as permitted by, and in accordance with, this Policy and applicable law.

DEFINITIONS:
Business Associate has the same meaning as the term "business associate" at 45 C.F.R. § 160.103.

KONZA means Kansas Health Information Network, Inc. which is the entity with whom the Participant has contracted to provide health information exchange and data analytics, data aggregation, and reporting services for health care providers in the state.

Custom Report means a Data Report that is not a Standard Report that is produced by KONZA in a format and content specifically requested by the Requestor following the Requestor's submission of a Purchase Order to KONZA.

Data Aggregation means the combining of Protected Health Information received by KONZA from one Participant with the Protected Health Information received by KONZA from another Participant to permit data analyses and reporting that relate to the Health Care Operations of the respective Participants.

Data Reporting and Analytics means the aggregation, analysis, and reporting to a Requestor by KONZA of the Protected Health Information that is exchanged through KONZA based on a Requestor's specific request.

Data Reports mean the work product resulting from the Data Reporting and Analytics that is delivered to the Requestor.

Data Use Agreement means an agreement which sets forth the permissible use of a Data Set and, in the case of a Limited Data Set, meets the requirements set forth at 45 C.F.R. § 164.514(e)(4).

De-Identified Data Set means information that excludes the specific identifiers set forth at 45 C.F.R. § 164.514(b)(2) and for which there is no knowledge that such information could be used to identify the subject of the information.

Health Care Operations has the same meaning given to the term "health care operations" at 45 C.F.R. § 164.501.

HIPAA-Compliant Authorization means a consent form for the use and disclosure of Protected Health Information that meets all of the requirements set forth at 45 C.F.R. § 164.508(c).

Identified Data Set means information which includes one or more of the direct identifiers set forth at 45 C.F.R. § 164.514(e)(2).

Individual means the person who is the subject of the Protected Health Information.

IRB or **Institutional Review Board** means a committee that has been formally designated to approve, monitor, and review biomedical and behavioral research involving humans, as defined and governed by 45 C.F.R. Part 46, implementing the provisions of the National Research Act of 1974.

Limited Data Set means information which excludes the specific direct identifiers set forth at 45 C.F.R. § 164.514(e)(2).

Participant means an individual or organization that has entered into a KONZA Participation Agreement.

Payment has the same meaning given to the term "payment" at 45 C.F.R. § 164.501.

Protected Health Information or **PHI** has the same meaning given to the term "protected health information" at 45 C.F.R. § 160.103.

Public Health means those activities and types of disclosures described at 45 C.F.R. § 164.512(b).

Purchase Order means a Statement of Work or Purchase Order executed by KONZA with its customer.

Requestor means a person or entity that requests Data Reporting and Analytics in accordance with this Policy. A Requestor can be either a Participant or a Third-Party Requestor.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Standard Report means those Data Reports and dashboards that are regularly produced by KONZA for Participants. A list of the types of Standard Reports that may be produced for Participants is set forth on Appendix A. The types of Standard Reports which are produced are updated from time to time to meet the needs of Participants.

Third Party Requestor means a Requestor that is not a Participant.

Treatment has the same meaning given to the term "treatment" at 45 C.F.R. § 164.501.

POLICY:

1. Compliance with Applicable Law. All requests for Data Reporting and Analytics by Requestors and the performance of Data Reporting and Analytics by KONZA must be in accordance with this Policy, applicable KONZA procedures, and applicable law.

2. KONZA Business Associate Agreements. To perform Data Reporting and Analytics, KONZA enters in Business Associate Agreements with its Participants and obtains the ability under each Business Associate Agreement it has entered into with its Participants to perform Data Aggregation services and to de-identify Protected Health Information in accordance with 45 C.F.R § 164.514(b).

3. Data Reports Comprised of an Identified Data Set. KONZA may perform Data Reporting and Analytics and provide Data Reports that are comprised of an Identified Data Set to Requestors for the following purposes, subject to the process and other restrictions set forth in this Policy, applicable KONZA procedures, and applicable law:

   A. Treatment;
   B. Payment;
   C. Health Care Operations;
   D. Public Health Activities;
   E. Research; and
   F. Any other purpose explicitly set forth in a HIPAA-Compliant Authorization obtained from each Individual whose Protected Health Information is included in the Identified Data Set.

4. Data Reports Comprised of a Limited Data Set. KONZA may perform Data Reporting and Analytics and provide Data Reports that are comprised of a Limited Data Set to Requestors if the Data Report will be used by the Requestor for Health Care Operations, Public Health, or Research purposes, subject to the process and other restrictions set forth in this Policy, applicable KONZA procedures, and applicable law.

5. Data Reports Comprised of a De-Identified Data Set. KONZA may perform Data Reporting and Analytics and provide Data Reports that are comprised of a De-Identified Data Set to Requestors, subject to the process and other restrictions set forth in this Policy, applicable KONZA procedures, and applicable law.

6. Connections to Other Health Information Exchanges. KONZA may connect to the federal eHealth Exchange and/or The Sequoia Project d/b/a Carequality® ("**Carequality®**"). In addition to the eHealth Exchange and Carequality®, KONZA may exchange Participant Data with other TEFCA QHINs and Participants.

7. Prohibited Use of Data. A Participant must limit its use of Standard Reports and Custom Reports as required by law and to the specific purposes indicated in any applicable Purchase Order. Any violation of this prohibition will be subject to the remedies and/or penalties set forth in this Policy and/or in a separate written agreement between the Requestor and KONZA.

8. No Further Disclosures. Unless otherwise authorized by KONZA, a Requestor may not further disclose a Data Report to any third party regardless of whether or not such disclosure would be permitted by applicable federal or state law. Any violation of this prohibition will be subject to the remedies and/or penalties set forth in this Policy and/or in a separate written agreement between the Requestor and KONZA.

9. Notification of an Impermissible Use or Disclosure. If a Requestor becomes aware that it has used or disclosed a Data Report in violation of this Policy, regardless of whether the impermissible use or disclosure was intentional or inadvertent, the Requestor must alert KONZA within one (1) hour of discovering information that leads the Requestor to reasonably believe that a breach as defined by applicable law may have occurred. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a breach has occurred, the Requestor must provide notice to KONZA. Failure to so timely notify KONZA will result in the remedies and/or penalties set forth in this Policy and/or in a separate written agreement between the Requestor and KONZA.

10. Remedies for Violations. In addition to any remedies set forth in an agreement between KONZA and a Requestor, if a Requestor violates this Policy, KONZA may deny any future requests for Data Reporting and Analytics made by the Requestor, as well as entities under common control or ownership as the Requestor. Further, because a violation of this Policy by the Requestor may cause substantial and continuing damage to KONZA (and its Participants), the value of which will be difficult or impossible to ascertain, KONZA reserves the immediate right to seek both temporary and permanent injunctive relief necessary to prevent the Requestor's violation of this Policy, without the need to prove damage or post bond.

11. Fees. Any fees that KONZA charges a Requestor are for Data Reporting and Analytics and not for Protected Health Information.

12. Record-Keeping Requirements. KONZA institutes and follows appropriate procedures for maintaining any version of this Policy for a period of seven (7) years after last use.

13. Internal Procedures. KONZA implements internal operating procedures and guidelines for carrying out its obligations set forth in this Policy.

References:

Internal: (insert any cross-referenced policies)

External:

1. HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164, Subparts C, D, and E.)

Security Override for Point-of Care Disclosure to Participants	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 006
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE
The purpose of this policy is to identify procedures to follow when Participants request access ("Requesting Participants") through KONZA to obtain health information from other Participants ("Disclosing Participants") for the care and treatment of patients (1) whose Protected Health Information (PHI) is blocked from being used or disclosed through KONZA either at the request of the patient or at the request of the patient's provider on behalf of the patient, and/or (2) whose PHI is protected under 42 C.F.R. Part 2 ("Part 2").

POLICY
KONZA does not use or disclosure any PHI of patients (1) whose Protected Health Information (PHI) is blocked from being used or disclosed through the KONZA either at the request of the patient or at the request of the patient's provider on behalf of the patient, and/or (2) whose PHI is protected under 42 C.F.R. Part 2 ("Part 2") **unless**

(1) The patient has signed a one-time authorization and consent authorizing use and disclosure of the patient's PHI at the point of care in and through KONZA, or,

(2) A patient's health information is necessary to treat the patient in a Medical Emergency (as defined below),

and, if applicable, the Requesting Participant obtains the patient's explicit consent to such disclosure pursuant to a Part 2-compliant consent form signed by the patient at the point-of-care.

When a Medical Emergency exists or a patient signs the one-time authorization and consent and, if applicable, a Part 2-compliant authorization form, in accordance with this Policy, Requesting Participants may utilize KONZA's Security Override to access and use the patient's health information through KONZA for the care and treatment of the patient at the point-of-care.

PROCEDURE
A. KONZA Participant Security Override: Granting Point-of-Care Access

1. Access. When using the KONZA web based portal, KONZA permits Requesting Participants to override access restrictions placed on certain patients' information in the health information exchange at the point-of-care in the following circumstances:

    a. Medical Emergency. Patient information may be disclosed by KONZA, on behalf of a Disclosing Participant, to a Requesting Participant that has a need for information about the patient for the purpose of treating the patient in a Medical Emergency; or

b. Receipt of Patient Consent. Patient information may be disclosed by KONZA, on behalf of a Disclosing Participant, to a Requesting Participant when the patient consents to a disclosure of his or her records by providing the Requesting Participant with a signed "Patient Consent and Authorization Form for Point-of-Care Disclosures" (the "POC Disclosure Form").

2. Limited Authorization; Time. A Requesting Participant's override access to the patient's restricted health information is authorized only for the date such access is requested by such Participant (i.e., the authorization expires at the end of the patient's care and treatment).

3. Read-only Format. KONZA provides access to the patient information in a "read-only/view-only" format such that the patient's information will not become part of the Requesting Participant's medical records for the patient when information is disclosed via an override at point-of-care treatment, unless such information is manually entered into the Requesting Participant's medical record for care documentation purposes, subject to the restrictions on redisclosure provided in this policy.

B. Medical Emergency ("Security Override")

1. General. A Requesting Participant's health care provider (the "Authorized User") treating a patient may encounter access restrictions placed on certain patients' information in the health information exchange at a patient's point-of-care.

2. Medical Emergency Access. Upon the determination by an Authorized User that a Medical Emergency exists at a patient's point-of-care, the Authorized User may override the KONZA access / security restrictions on a patient's information without the patient's consent (i.e., break the glass).
"Medical Emergency", as used in this policy, is defined as a bona fide medical emergency in which the patient's prior informed consent cannot be obtained. Any health care provider who is treating the patient for a medical emergency can make this determination.

   a. Override. When the Authorized User is prompted by the KONZA system to select a choice as to why the override was performed, the Authorized User will select and certify that the patient was experiencing a Medical Emergency.
   b. Entire Record. Once the override is performed, all patient's information available in KONZA, which may include Part 2 health information necessary to address the Medical Emergency, may be released through KONZA to Participant's Authorized User.

3. Part 2 Documentation /Notice Requirement. Because Part 2 requires Part 2 programs to document certain information into a patient's record when a disclosure is made during a Medical Emergency and because other Participants may want to document certain information into a patient's record when a disclosure is made during a Medical Emergency, KONZA utilizes its auditing capabilities and daily audit logs to provide the appropriate information and notice of the disclosure to KONZA's Disclosing Participants.
   a. In circumstances where a patient's information is disclosed in a Medical Emergency, without patient consent such an occurrence is flagged in the KONZA daily audit log.
   b. Relevant to the specific disclosure, KONZA will gather the information set forth below and thereafter provide such information in the form of a notice to the applicable Disclosing Participant's compliance officer or inclusion in their patient records as soon as possible after the disclosure occurs.
   c. The information included in the notice to the Disclosing Participants includes:
      i. The name and affiliation of the Authorized User receiving the patient's health information;

      ii. A statement that KONZA made the disclosure through the health information exchange;

iii. The date and time of the disclosure; and
iv. The nature of the emergency.
v. If the disclosure included Part 2 information the Part 2 program will be notified of the disclosure.

d. Disclosing Participant will retain a copy of the patient's Medical Emergency disclosure information in its respective records for a period of seven (7) years. KONZA retains the right to audit Disclosing Participant's records to obtain and/or verify Disclosing Participant's documentation of the Part 2 disclosure notice.

C. Receipt of Patient Consent

1. General. An Authorized User treating a patient may encounter access restrictions placed on certain patients' information in the health information exchange at the patient's point-of-care.

2. Patient Authorization Form and Access. When a patient does not present with a Medical Emergency and access to the patient's health information is restricted, the Authorized User may present a patient (or his/her authorized representative) with the POC Disclosure Form to obtain the patient's authorization for the Requesting Participant and its Authorized Users to override the restriction. The POC Disclosure Form is Part 2-compliant.
   a. Presentation of Consent Form. Authorized User will explain to the patient the nature of the POC Disclosure Form and the purpose of the Authorized User's access and disclosure. Authorized User will provide the patient with time to: (i) read the POC Disclosure Form, (ii) ask questions, and (iii) either execute or refuse to execute the POC Disclosure Form. If the patient is a minor, the POC Disclosure Form should be signed by both the minor patient and the minor patient's parent or guardian. Note: Wet signatures, facsimiles or photocopies of signatures or electronic signatures are valid.
   b. Refusal to Execute. If the patient refuses to sign the POC Disclosure Form, the Authorized User will state that he/she cannot access the medical record via KONZA. Subsequent treatment or care will be provided as determined by the Authorized User. The patient's refusal to sign the POC Disclosure Form shall be documented by the Authorized User in the patient's record and the patient will not be discriminated against because of the refusal.
   c. Consent Received. If the patient executes the POC Disclosure Form, the Authorized User has received explicit patient consent to override KONZA's restriction and will continue to follow the access procedures provided in this section.
   d. Access. When the Authorized User is prompted by the KONZA system to select a choice as to why the override was performed, the Authorized User will select and certify that he/she has received explicit patient consent pursuant to the POC Disclosure Form.
   e. Records Released. In accordance with the POC Disclosure Form, a patient's entire medical record, which may include information protected by Part 2, may be released through KONZA to the Authorized User in a read-only format for use in the patient's care and treatment provided at the point-of-care.

3. Documentation. Requesting Participant will retain a copy of the patient's executed POC Disclosure Form in its respective records for a period of seven (7) years. KONZA retains the right to audit Requesting Participant's records to obtain and/or verify the existence of executed POC Disclosure Forms.

4. Redisclosure. The POC Disclosure Form is limited to obtaining health information for the treatment and care of patient at the point-of-care that day by the Authorized User. Part 2 restricts health information containing Part 2 information to be redisclosed when such information is obtained pursuant to a Part 2-compliant consent form. Because health information protected by Part 2 may be disclosed to the Requesting Participant upon receipt of an executed POC Disclosure Form, the Requesting Participant is informed by this Policy that the PHI disclosed to the Requesting Participant is subject to the following notice:

"Some of the information disclosed to you may be protected by Federal confidentiality rules (42 C.F.R. Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. Federal law restricts any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients."

Accordingly, should the Requesting Participant or Authorized User wish to further disclose a patient's information beyond the point-of-care treatment being provided, another separate and distinct Part 2-compliant consent form must be presented to and executed by the patient prior to redisclosure by the Requesting Participant/Authorized User, unless an exception under Part 2 applies.

D. Enforcement, Training and Revisions

1. KONZA Responsibilities.
   a. KONZA will require Requesting Participants and Authorized Users to follow this policy and procedure, and will assist in the training and education of Requesting Participants/Authorized Users (as necessary).
   b. KONZA will support Requesting Participants and Authorized Users with the appropriate technical override capabilities to access necessary patient information at point-of-care.
   c. KONZA will perform the audits / audit logs required to obtain Part 2 program notice information and provide such information to Part 2 program Disclosing Participants as required by law.
   d. KONZA will notify the Requesting Participant's compliance officer, or such other administrator in a similar position, of the Requesting Participant's access to and receipt of restricted patient health information via KONZA.
   e. KONZA will maintain and make any necessary revisions to the template POC Disclosure Form.
   f. KONZA will confirm this policy and procedure remains up to date with the capabilities of KONZA's health information exchange, and the requirements of state and federal law.

2. Participants' Responsibilities.
   a. Participants agree to identify Authorized Users that will have security override access.
   b. Requesting Participants agree to provide training and education to Authorized Users to confirm access to restricted patient health information via KONZA is in accordance with KONZA's policies and procedures.
   c. Requesting Participants and Authorized Users will be responsible for certifying that the Authorized User has accessed restricted information either for a Medical Emergency or pursuant to receipt of an executed POC Disclosure Form.

Participants agree to maintain and retain patient records and documentation sufficient to establish that the security override was appropriate under this policy.

Restrictions of Use of Sensitive Information	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 007
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE

Federal and state laws may impose heightened privacy requirements regarding the use and disclosure of certain types of protected health information that may be considered particularly private or sensitive to a patient (hereafter, Sensitive Health Information.) Depending upon the permitted purpose(s) for which Sensitive Health Information is being disclosed, the law may require a patient prior to disclosure through Kansas Health Information Network, Inc. to specifically authorize in writing a particular disclosure of Sensitive Health by signing a document that contains the required, legal elements. The purpose of this Policy is to identify Participants' obligations regarding the disclosure of Sensitive Heath Information through KONZA.

POLICY

The Participant is responsible for obtaining from the patient any special authorizations required by federal or state law PRIOR to disclosing Sensitive Health Information through KONZA. In certain situations regarding certain types of Protected Health Information, federal and state law may impose more restrictive privacy rules to such sensitive Protective Health Information (Sensitive Health Information) than HIPAA. Depending upon the purposes for which Sensitive Health Information is being sought, the law may require a patient prior to disclosure through KONZA to specifically authorize in writing the disclosure of Sensitive Health Information by signing an authorization for disclosure that contains certain elements. If such a special authorization is required by law, Participants shall not disclose through KONZA Sensitive Health Information that requires the execution of a specific, written authorization unless Participant has obtained any required authorization for disclosure from the patient prior to disclosing the Sensitive Health Information through KONZA. Responsibility for restricting the disclosure of Sensitive Health Information through KONZA without any legally, required authorization from the patient will reside with the Participant. The transmitting Participant shall obtain an appropriate authorization from the patient in accordance with applicable law prior to disclosing or re-disclosing Sensitive Health Information through KONZA.

Sensitive Health Information may include but is not limited to:

- Substance abuse records
- Mental health and psychotherapy records
- Genetic testing information
- HIV/AIDS information
- Developmental disability records
- Communicable disease information

Policy Governing Data for Patients who Self-Pay for Healthcare	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 008
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date:July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

Responsibility: Kansas Health Information Network, Inc. Members who provide direct care to patients (Covered Entity)

General Information:

The Kansas Health Information Network, Inc. shares patient data as allowed under HIPAA for treatment, payment and health care operations (TPO) as well as secondary data uses outlined in the Secondary Data Use Policy. This includes sharing data with health plans for their members.

KHIN does not collect financial data from its members. KHIN has no knowledge of the manner in which a patient resolved their financial obligations to the health care provider and relies upon the Covered Entity to block any clinical information that should not be shared with a health plan.

KHIN Member Responsibilities:

1. KHIN members must omit or block any clinical information where the patient self-payed for the services rendered.

2. If the technology at the facility is not equipped to comply with this requirement then the KHIN member must opt the patient out of data sharing in the exchange.

3. KHIN Members may refer patients to opt themselves out of sharing data through the exchange website.

Information Blocking	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 009
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2) 45 CFR part 171*** Policy Cross Reference(s):
Effective Date:July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 17, 2024

Responsibility: Kansas Health Information Network, Inc.

General Information:

Advances in health information technology has promoted the expansion of electronic health information (ePHI) and made the ePHI more accessible through health information exchange. In 2016, the passage of the 21st Century Cures Act (Cures Act) made sharing of electronic information the expected norm in health care and authorized the Secretary of Health and Human Services (HHS) to identify "reasonable and necessary activities that do not constitute information blocking."

As defined in the Cures Act, Kansas Health Information Network, Inc. operates as a Health Information Network. As documented in these HIE Policies and Procedures, Kansas Health Information Network, Inc. responds and exchanges information for HIPAA permitted exchange purposes.

Policy

1. Kansas Health Information Network, Inc maintains authority to evaluate requests for information across the eight (8) exceptions to information sharing.
   1.1. Preventing Harm Exception
   1.2. Privacy Exception
   1.3. Security Exception
   1.4. Infeasibility Exception
   1.5. Health IT Performance Exception
   1.6. Content and Manner Exception
   1.7. Fees Exception
   1.8. Licensing Exception

2. All requests for ePHI sharing are evaluated against the Kansas Health Information Network HIE Policies and Procedures along with the Privacy and Security Policies.
3. Individuals can request access to their information through a Personal Health Record. Accounts can be requested through the KONZA HelpDesk.

Dispute Management and Participant Enforcement	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 010
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

Responsibility: Designated Network Governance Body

The KONZA Management Committee is comprised of a subset of the Designated Network Governance Body.

KONZA executes contracts with Participants binding them to contractual, legal, and technical obligations of the Network. Disputes can be generated between the actors listed below. All disputes, regardless of actors, will follow the Dispute Management Process listed below. This includes the following;

1. between Participants and Subparticipants
2. between a Participant or Subparticipant and the Kansas Health Information Network, Inc. dba KONZA
3. between external networks and the Kansas Health Information Network, Inc. dba KONZA

In the event that KONZA is designated as a QHIN under TEFCA, KONZA will adhere to the Dispute Resolution process defined in the Common Agreement and administered by the RCE.

This process addresses disputes and participant enforcement across the following topics:

1. Governance of Network
2. Privacy or Security Practices
3. Data Breaches
4. Policy requirements
5. Legal requirements
6. Technical requirements
7. Other

Dispute Management and Participant Enforcement Process

1. Submission and Documentation of Disputes
   - 1.1 President and CEO will serve as primary actor on behalf of the Network.
   - 1.2 The Privacy and Security Officer (PSO) is the primary point of contact for any Disputes.
   - 1.3 All disputes must be submitted in written form to the PSO.
   - 1.4 PSO will document in HIPAA Complaint Log
   - 1.5 PSO will contact the individual making the complaint within one business day of receiving notice of the complaint. Contact will be made using the most efficient and immediate means available, preferably by email. The Privacy Security Officer (PSO) will document the date and time of their response on the HIPAA Complaint Log. If a voice mail is left, he/she will continue to pursue direct communication until it occurs.

2. Investigation of Disputes
   - 2.1 The dispute will be routed to the HIPAA Risk and Security Committee for full investigation.
   - 2.2 The dispute will be reviewed with any individual(s) associated with Kansas Health Information Network, Inc. dba KONZA that have been identified
   - 2.3 Reporting of Disputes are done immediately to the President and CEO. The President will then communicate to the Management Committee the nature of the dispute.
   - 2.4 HIPAA Risk and Security Committee, in conjunction with the Management Committee, will make a recommendation on the level of severity of the dispute, following the levels defined below.

2.4.1 Level One (Carelessness): An unintentional or careless violation by the Participant. The suggested actions in response to a Level One violation include verbal and written warnings and/or additional training.

2.4.2 Level Two (Curiosity or Concern (no personal gain)): An intentional violation or inappropriately using the KONZA but for purposes unrelated to personal gain. The suggested sanctions for a Level Two violation include those set forth for Level One, as well as suspension or probation related to the applicable Participant User's access to the KONZA, a written corrective action plan, and follow up to determine if such actions are addressing the issue(s).

2.4.3 Level Three (Personal Gain or Malice): An intentional violation or inappropriately using KONZA for personal gain or with malicious intent. Suggested actions for a Level Three violation include suggested immediate termination of the Participant's User's access to KONZA, and termination of the Participant Agreement (if immediate corrective action is not taken by the Participant).

2.4.4 Level Four (Suspected Criminal Acts or Activity): A suspected criminal violation. In such an event, KONZA will contact law enforcement and appropriate authorities immediately. Suggested actions for a Level Four violation include suggested immediate termination of the Participant's User's access to KONZA, and termination of the Participation Agreement.

3. Dispute Resolution and Enforcement
   - 3.1 Sanctions are applied by level of severity as defined above.
   - 3.2 For any dispute categorized as a Level 1 or Level 2 severity, the CEO and President, who may delegate to the COO as needed, has the authority to resolve and rule on the dispute.
     - 3.2.1 The Management Committee will be informed on the resolution of the dispute.
   - 3.3 For Level 3 or 4 disputes, the Management Committee of the Board has the authority to resolve and rule over such disputes. Voting and quorum requirements are inherited from the Bylaws. A majority of the Directors on the Management Committee will constitute a quorum for the transaction of business.
     - 3.3.1 Upon the Management Committee completing a preliminary investigation and determining that there is a substantial likelihood that a Participant's acts or omissions constitute a Level 3 or Level 4 severity dispute; the Management Committee will consider suspension or recommendation of termination of the Participant.
     - 3.3.2 Upon the termination recommendation by the Management Committee, the Designated Network Governance Body will meet for a final ruling
       - 3.3.2.1 A quorum of the Board is required.
       - 3.3.2.2 A majority vote for termination is required.
       - 3.3.2.3 If a majority vote is not achieved, the dispute is reverted back to the Management Committee for suspension and Plan of Correction
     - 3.3.3 Upon the decision to suspend or terminate, the Management Committee shall authorize the CEO to immediately suspend or terminate the Participant's connection and within twelve (12) hours of suspending or terminating a Participant.
       - 3.3.3.1 provide Notice of such suspension or termination to all Participants; and
       - 3.3.3.2 provide to the suspended or terminated Participant a written summary of the reasons for the suspension or termination; and
       - 3.3.3.3 if appropriate, provide information on a Plan of Correction
   - 3.4 PSO will document the final rulings in the HIPAA Compliant Log, with a resolution date.

4. Report to the Designated Network Governance Body
   - 4.1 All disputes will be reported to the Designated Network Governance Body
   - 4.2 The disposition of all disputes will be reported to the Designated Network Governance Body
   - 4.3 The Designated Network Governance Body will be notified of any actions taken by the RCE or KONZA for dispute management or other participant enforcement for reasons for non-compliance. Such actions may include and are not limited to suspension or termination.
5. Plan of Correction
   - 5.1 As part of the Dispute Resolution, a Plan of Correction may be assigned.
   - 5.2 The Plan of Correction includes tasks and actions needed to bring the Participant into full compliance with the flow down conditions and terms.
   - 5.3 Resolutions with a defined Plan of Correction also include actions if violations occur.
   - 5.4 The PSO has delegated authority to monitor and manage the associated milestones defined in the Plan of Correction

5.4.1 If at any time, the Plan of Correction is violated, the dispute is again routed to the appropriate decision-making authority (3.3 and 3.4 above).

5.5 Removal or reversal of Level 3 or Level 4 sanctions (i.e., reinstatement) require approval from the Management Committee of the Board

6. Appeals of disputes
   6.1 Either party has the opportunity to request an appeal of the dispute resolution within 2 calendar weeks of the resolution date if additional information is available and has not been considered in the initial ruling.
      6.1.1 Appeals of Level 1 or Level 2 disputes are routed to the Management Committee of the Board.
      6.1.2 Appeals of Level 3 or Level 4 disputes resulting in suspension are routed to the Designated Network Governance Body.
   6.2 Appeals for termination may be requested after 6 months from the dispute resolution date.
   6.3 Requests for appeals is sent in writing and documented in the HIPAA Compliant Log

7. Participant Enforcement
   7.1 The DNGB makes the final determination of any termination of Participant for any reason.
   7.2 The Management Committee will make any decisions on the suspension of a Participant for any reason.
   7.3 Participants may request a voluntary suspension or termination of participation in the Network.
      7.3.1 Such requests are sent if the Participant realizes they are out of compliance with flow down terms and conditions.
      7.3.2 Participants must put the request in writing.
      7.3.3 The Designated Network Governance Body will be informed of such actions.

Data Breach Response Policy	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 011
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE

This policy has been created to internally assist KONZA in management of security incidents or data breaches. This Policy is in addition to, and not a replacement of, Participant's breach notification, mitigation, and sanction policies and procedures. Participants should abide by their own policies and procedures in addition to this policy.

DEFINITIONS

Security Incident: Warning received from Participant, KONZA staff, or through system monitoring that there may be a threat to data or system security.

Security Event: Confirmed change in operations that violated security policy(s).

Data Breach: as defined in 45 CFR § 164.402

POLICY

1. In accordance with the Participant Agreement, Business Associate Agreement, and KONZA Policies, KONZA may take action against a Participant for failure by the Participant to comply with applicable laws and policies related to the protection of PHI.

2. The Participant Agreement provides KONZA the ability to immediately terminate the applicable Participant Agreement in such an instance, and, therefore, this policy provides guidance to KONZA to determine the proper consequences of a Participant's non-compliance.

3. KONZA will follow the terms set forth in this policy to determine what actions, up to and including termination of the Participant Agreement, need to be taken against a Participant for any such failure.

4. In the event that KONZA becomes aware or receives notification that a Participant has breached or potentially breached an obligation related to the confidentiality of PHI, the Dispute Management and Participant Enforcement shall be used to manage the investigation and next steps.

PROCEDURE

1. Internal KONZA staff shall report any suspected security incidents to the KONZA HIPAA Risk and Security Committee with as many details as possible.
2. External participants should communicate any suspected Security Incidents to the KONZA Privacy and Security Officer (PSO).
3. The HIPAA Risk and Security Committee shall investigate and determine the impact and level of risk

of suspected vulnerability. The following points are determined as part of the investigation:

a. The number of patients affected;
b. The degree of potential harm to the patient(s);
c. Whether the action was negligent or purposeful;
d. Whether the action caused harm or is likely to cause harm;
e. The actions taken by the Participant in response to the non-compliance and their effectiveness to remedy the situation; and
f. Whether the Participant has had other PHI violations in the past, and how the Participant responded in those situations.

4. The HIPAA Risk and Security Committee will report to the CEO, who, in turn completes reporting to the Designated Network Governance Body.
5. The PSO shall coordinate internal and external communication regarding the investigation, outcome, and next steps.

Mitigation Policy	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 012
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE

The purpose of this policy is to require participants and KONZA to mitigate with appropriate remedial action in the event an unauthorized use or disclosure occurs.

POLICY

Each Participant shall implement a process to mitigate, and shall mitigate and take appropriate remedial action, to the extent practical, any harmful effect that is known to the Participant of a use or disclosure of Protected Health Information (PHI) involving KONZA products in violation of applicable laws and/or regulations and/or the Policies and Procedures by the Participant, or its workforce members, agents, and contractors.

The Participant shall notify KONZA if information included in KONZA products was used or disclosed in violation of the law, the Participant Agreement, or KONZA policies and procedures. Participant shall comply with all applicable laws requiring notification or other steps in the event of inappropriate disclosure of information pertaining to an individual.

KONZA shall notify Participants if information they provided was used or disclosed in violation of the law, the Participant Agreement, or KONZA policies and procedures. KONZA shall implement a process to mitigate, and shall mitigate and take appropriate remedial action, to the extent practical, any harmful effect that is known to the KONZA of a use or disclosure of PHI involving KONZA products in violation of applicable laws and/or regulations and/or the Policies and Procedures by KONZA, or its workforce members, agents, and contractors.

Auditing and Reporting Policy	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 013
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

Definitions:

Audit Log: The term audit log shall mean a record of actions performed on data. Examples are creation, queries, views, additions, deletions, and changes.

Audit Trail: The term audit trail shall mean a record that shows who has accessed a computer system, when it was accessed and what operations were performed.

Breach: The unauthorized acquisition, access, use or disclosure of Unsecured Protected Health Information in a manner not permitted by the Privacy Rule or Security Regulation (45 CFR 164.402) which compromises the security or privacy of such Protected Health Information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the individual.

Electronic Protected Health Information (ePHI): The term Electronic Protected Health Information (ePHI) shall mean any protected health information (PHI) which is created, stored, transmitted, or received electronically.

Participant: The term "Participant" shall mean an organization registered with KONZA who is a party to the Data Sharing Agreement and approved to act as a Data Provider and/or Data Recipient.

Protected Health Information (PHI): The term Protected Health Information (PHI) shall have the meaning ascribed to it by 45 CFR 160.103, and shall include, but not be limited to, written or electronic information relating to the diagnosis, treatment, test, prognosis, admission, discharge, transfer, prescription, claims and/or other data or information implicitly or explicitly identifying a patient to whom items or services are provided by a Participant, which information is provided, stored, or accessed by a Participant in connection with the EHR system.

Unsecured Protected Health Information: The term Unsecured Protected Health Information shall mean Protected Health Information that has not been secured through the use of technology or methodology standards as provided by federal law.

Purpose:

Effective logging and audit practices are essential safeguards as electronic protected health information (ePHI) is shared at the regional, state, and national levels. KONZA will strive to act in accordance with HIPAA, HITECH, and federal and state regulations when ePHI is accessed. To detect any misuses of information, inappropriate access, or disclosures of ePHI, it is important to have this set of logging and auditing practices in place as is expected under the Privacy Rule. Having effective auditing and logging practices can foster trust among individual patients and the general public in knowing that their data is being used only in appropriate ways.

KONZA will implement technical, physical, and administrative safeguards to protect health information as

outlined in the HIPAA provisions, 45 CFR 164.530(c)(1)

Policy:
It is the policy of the KONZA that a system of accountability is an integral component in the stewardship of ePHI, and that ePHI will be accessed strictly for the purposes of treatment. This access shall be limited to authorized individuals with a valid need-to-know in the performance of their regular job duties.

Procedure:

Audit Logs

1. The KONZA Executive Director or designee will generate and store all audit logs for Participants using the web-based portal. Participants viewing the HIE from within their EHR shall be responsible for their own audits of HIE access.

2. All original audit logs will be held in a secure location and in a tamper proof format and may only be accessible by the KONZA Executive Director or designee.

3. Audit logs shall be maintained by KONZA for at least three (3) years.

4. The KONZA Executive Director or designee will review the monthly reports for suspicious activity and disseminate appropriate and relevant findings to the appropriate Participant's Privacy Officer for further review and investigation.

5. Upon request, KONZA shall provide to each Participant statistical summaries indicating the number of accesses to the requesting Participant's own PHI by accessing site and including a list of all queries to the EHR system by patient names and date of birth.

6. Participant or customer shall cooperate with KONZA in any audit, including, but not limited to, providing KONZA access to any data, records or system reasonably necessary for KONZA to evaluate the Participant's compliance, making personnel available to discuss the Participant's processes and procedures, and making space available on-site for KONZA to conduct the audit.

Auditing Process

1. During the first week of the month, audit log information will be provided to Participants by KONZA reflecting the previous month's activity. The data will be provided in standard format (e.g. txt, csv, xls, etc), and will include the following data elements:
   - User(s) responsible for the audit event
   - User Location/Department
   - Date and time of the audit event
   - Date audit report generated
   - IP address of the computer used
   - Patient Name
   - Medical Record Number
   - Vault viewed
   - Event type viewed

1. The Participant shall review and investigate all reported suspicious activity and determine whether the access was appropriate or inappropriate. Results of the investigation shall be reported back to KONZA.

   a. Suggested Guidelines for Reviewing Monthly Audit Reports - Suspicious Activity
      - Includes same last name (i.e., user Mary Smith accessing Robert Smith)
      - Patterns of usage (was same patient accessed repeatedly)
      - Employee accessing another employee record (may need to reference Participant employee list)

2. If the Participant investigation verifies that a breach has or may have occurred, user access shall be temporarily suspended until completion of a full investigation.

Audit Alerts

KONZA shall also develop audit alerts and processes for reporting non-standard activity. Audits shall be run monthly and reported to Participants and may include any or all of the following:

1. Routine Audits
   - Random selection of users by Participant
   - New user activity for 90 days
   - Users with no activity for 90 days

KONZA Responsibilities

1. KONZA will identify suspicious activity and provide Participant or customer with the necessary information about the inappropriate use, disclosure or access of PHI.

2. KONZA will support any follow-up on the suspicious activity with the appropriate Participant.

3. KONZA will provide Participants assistance from KONZA in the procurement of further detail not included in the standard audit log information. Additional ad hoc reports can be requested from and defined by the HIE as needed.

4. KONZA will require that each Participant implement a process to mitigate and take appropriate remedial action.

5. KONZA will require that each Participant provide timely documentation to support their investigation.

6. KONZA will follow all Privacy and HITECH Regulations on breach notifications.

Participant Responsibility

1. Participant will be responsible to inform KONZA of any suspicious activity.

2. Each Participant agrees to enforce the confidentiality provisions of the Data Sharing Participation Agreement by appropriately disciplining individuals within each Participant's organization who violate the confidentiality of PHI pursuant to each Participant's respective confidentiality and disciplinary policies. Such discipline may include, but shall not be limited to warnings, suspension, termination, and/or modification, suspension, or revocation of the Authorized User's access to the EHR System.

Technical Framework Policy	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 014
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

I. Purpose

The Technical Framework Policy defines the administrative oversight and governance provided by the Designated Network Governance Body and the Technology Vendor Review Committee for the KONZA Designated Network.

II. Policies and Procedures

1. The Technical Vendor Review Committee is responsible for ongoing evaluation and oversight of our technology vendors and the services they provide.

2. The Technical Vendor Review Committee is responsible for making recommendations to the Sr Leadership team for changes (additions, removals, or modifications) along with status updates of vendor performance against contracted services.

3. The Sr Leadership team evaluates the recommendations of the Technical Vendor Review committee and is responsible for final recommendations to the Designated Network Governance Body regarding changes to the Technical Framework.

4. Designated Network Governance Body approves all material changes to the Technical Framework.
    a. Material change is defined as included but not limited to
        i. Change in vendor
        ii. Addition or deletion of technical products

5. The Designated Network Governance Body (DNGB) can raise technical compliance issues or concerns.
    a. Such concerns are routed to the CEO
    b. The CEO will work to resolve all concerns and report back to the DNGB in a timely manner.

6. Any non-compliance of the Technical Framework Policy is addressed through the Dispute Management and Participant Enforcement policy.

Security Password Policy for Participants	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 015
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE

The purpose of this policy is to outline password policies for use with the web-based portal and indicate the responsible agency for Participant Authorized User Logon-ID and password maintenance for Kansas Health Information Network, Inc. d/b/a KONZA.

POLICY

Each "Authorized User" is responsible for the proper use of his or her account and any activity conducted with it. This includes choosing safe passwords, protecting them, and reporting any inappropriate access to data.

a. A Logon-ID is issued to an individual.
b. The individual to whom the Logon-ID is issued is responsible and accountable for the use of the Logon-ID.
c. Use of a Logon-ID by an individual, other than the one to whom the Logon-ID is issued, is considered a security violation.
d. A password protects against the misuse of a Logon-ID. The initial password that is associated with a Logon-ID must be changed by the user when the user logs onto the system for the first time.
e. A password must be kept secret. A password shall not be divulged to another individual. Passwords must not be placed where they could be easily seen or found.
f. Passwords for Logon-IDs are forced to automatically expire by the security software. Logon-ID password expiration shall be at regular intervals specified by KONZA.
g. Password length must be a minimum of seven (7) characters.
h. Password cannot be the same as the Logon-ID
i. Passwords must be changed every 180 days.
j. Passwords must contain characters from at least three (3) of the following four (4) classes:
    1. Upper case letters (A, B, C, ….Z)
    2. Lower case letters (a, b, c, ….z)
    3. Numbers (0,1, 2, …9)
    4. Non-alphanumeric ("special characters") such as punctuation symbols
k. Passwords may not contain your user name or any part of your full name.
l. Password history is kept to prevent the reuse of a specified number of past passwords. A previous password cannot be reused within the past 12 months.
m. Six (6) invalid attempts to enter a Logon-ID and password will result in an account lockout.
n. Passwords can be audited periodically for compliance by using automated password-cracker software.

User Access	
Kansas Health Information Network, Inc. d/b/a KONZA National Network Policies & Procedures	Policy #: 016
Section: ***One*** Subject: ***KONZA Policies***	Related Law(s): ***45 CFR §164.308(a)(2)*** Policy Cross Reference(s):
Effective Date: July 8, 2020	Last Update: July, 2022
Approved by: KHIN Board of Directors	Approval Date: July 13, 2023

PURPOSE

The purpose of this policy is to identify procedures by which Kansas Health Information Network, Inc. d/b/a KONZA and Participants manage the granting and removing of access privileges for Authorized Users of KONZA through the web-based portal.

POLICY

Each Participant in KONZA will be required to register Authorized Users with KONZA. Only Authorized Users shall be granted access to the KONZA. Users for each Participant will be managed by a formal requesting process, in which an authorized request to add or remove an Authorized User is sent to KONZA by the Participant.

Client Administrators

1. Each Participant must designate a Client Administrator who can authorize User Access Forms from individuals affiliated with the Participant to have access to the KONZA.

2. The Client Administrator will approve each User prior to submitting the Authorized User Form to KONZA.

Requesting Access

1. Each Client Administrator must complete the Authorized User Access before access to KONZA is granted. The User Access form will be sent to the KONZA Help Desk.

2. KONZA will review and process each User Access form as appropriate. Approved Users will be issued a User identifier and password. New User ID's and passwords will be sent to the Client Administrator at their KONZA Direct email.

3. The Participant shall be responsible for and oversee the implementation and use of the User identifier and any other measures appropriate to the Authorized User.

Access Levels

The access rights will be based on standard access profiles (see below).

Full Data Access: For each User with this access level, a User can see the visit and patient information of all patients if the patient has chosen to participate in the health information exchange. Additionally, patient data may be available if the patient has chosen not to participate in the health information exchange but either gives consent at the time of care or is having a life-threatening emergency subject to any applicable policies and procedures and the Participant Agreement.

Standard Data Access: For each user with this access level, a User can see the visit and patient information of those patients, except for patients that have chosen not to participate in the health information exchange. The User will not be able to view the protected health information of these

patients.

No access: The User cannot see any patient information.

A User can only have one of the above Data Access levels for each vault within the KONZA.

Functional Access Levels:

General User: User can view patient information within the KONZA. subject to their Vault Data Access level.

Health Information Management (HIM) User: User will have Full Data Access, the ability to manage documents and run clinical reports.

Security Override: User will be able to Override the patient's choice for Global Opt-Out. The User will identify a choice as to why the Override was performed. This action is identified on the Audit Reports.

Authorized Users

1. Each Participant agrees to restrict access to KONZA and use of KONZA's services to only those Authorized Users identified by the Participant and approved by KONZA.

Current Valid List of Authorized Users

1. Each Participant will be responsible for maintaining with KONZA a current valid list that contains the Client Administrators and all its Authorized Users. KONZA and each Participant will validate this list semi-annually.

2. KONZA will provide a list of currently Authorized Users for the Participant every six months.

3. The Participant will reply within ten (10) business days confirming and providing any updates for such list.

4. If Participant fails to respond within the designated time period, KONZA may suspend Participant's access to KONZA until the list is confirmed.

Responsibility for Conduct of Participant and Authorized Users

1. Participant shall be solely responsible for all acts and omissions of the Participant and all acts and omissions of the Participant's Authorized Users and all other individuals who access the EHR system and/or use KONZA Services either through the Participant or by use of any password, identifier, mechanism, or log-on received or obtained from the Participant or any of the Participant's Authorized Users.

2. All Authorized Users will follow all HIPAA rules and regulations when accessing patient data. KONZA recommends training the User with the supplied language. (Exhibit A)

Access Removal

1. Each Participant will promptly notify KONZA of need to remove and inactivate an Authorized User from its list of Authorized Users, including notification when a staff member or Authorized User is no longer employed by Participant.

2. Any violation by an Authorized User of the Data Sharing Participation Agreement, the Participant's Registration Agreement and the Policies and Procedures of KONZA may result in suspension or termination of the Authorized User's access to KONZA.

3. Participant shall comply with KONZA's policies and procedures regarding the termination of employment, termination of affiliation of an Authorized User or other removal of an Authorized User of Participant.

Suggested Language to Include in HIPAA Training Materials

Related to Participation in KONZA

_____ (Name of hospital/practice) participates in KONZA. KONZA provides the mechanism for sharing health-related information in a secure manner while protecting the confidentiality of the information among health care stakeholders. The exchange supports continuity of care and reduces duplicative procedures and paperwork.

As an employee of _____ you may have access to KONZA. It is important to note that HIPAA limits access to health care data to only that data necessary to accomplish the reason for access. This is called the "minimum necessary requirement." Access to data through KONZA is restricted based on the type of entity making the request. For example, a physician providing care in an emergency room will have greater access to the data than an admitting clerk.

_____Hospital/practice will conduct regular and ongoing audits of who accessed KONZA and for what purpose. In addition, KONZA will conduct random audits of access, and the state regulatory body may conduct audits as needed for compliance purposes.

Non-compliance with the minimum necessary rule and unlawfully accessing information will result in severe penalties. Under federal law, the penalties can extend up to a range of $250,000 or more with repeat/uncorrected violations extending up to $1.5 million or more.