OKLAHOMA STATE HEALTH INFORMATION NETWORK AND EXCHANGE

Table of Contents

PARTICIPATION AGREEMENT

THIS PARTICIPATION AGREEMENT ("PARTICIPATION AGREEMENT") IS MADE BY AND BETWEEN THE OKLAHOMA HEALTH CARE AUTHORITY (OHCA) d.b.a. THE OKLAHOMA STATE HEALTH INFORMATION NETWORK AND EXCHANGE (OKSHINE) AND _____ ("PARTICIPANT"). THE EFFECTIVE DATE FOR THIS PARTICIPATION AGREEMENT IS _____ ("EFFECTIVE DATE").

OKSHINE will provide, and Participant accepts services described in Exhibits A-F, as applicable. Participants in the Network include data recipients that will access data through OKSHINE and data suppliers that will provide data through OKSHINE.

Participant will participate in the transmission of data through OKSHINE and the submission or use of such data, as applicable, subject to this Participation Agreement and its Exhibits.

This Participation Agreement includes, and incorporates by reference:

Exhibit A – Terms and Conditions of Participation;

Exhibit B – Primary Contacts and Address for Notice;

Exhibit C – HIPAA Business Associate Agreement;

Exhibit D – Annual Participation Fees

Exhibit E – OKSHINE Available Services;

Exhibit F - OKSHINE Policies and Standards found at https://oklahoma.gov/ohca/okshine/resources.html

PARTICIPANT

BY:_____[Individual Authorized to sign on behalf of Participant]

_____[TYPED OR PRINTED NAME]

TITLE: _____

DATE: _____

OKSHINE

BY:_____[SIGNATURE]

Carter Kimble
Executive Director
Oklahoma State Health Information Network and Exchange (OKSHINE)
4345 N. Lincoln Blvd., Oklahoma City, OK 73105
P: (405) 564-4715
E: carter.kimble@okhca.org

DATE: _____

EXHIBIT A - TERMS AND CONDITIONS OF PARTICIPATION

SECTION 1 - DEFINITIONS

Terms used, but not otherwise defined, in this Participation Agreement shall have the same meaning as those terms in 45 C.F.R §§ 160.103 and 164.501; 42 U.S.C §300jj and 45 C.F.R. §171.10

1.1 "21st Century Cures Act" means 21st Century Cures Act: Interoperability, Information Block, and the ONC Health IT Certification Program published May 1, 2020.

1.2 "Administrative User" means an individual who is an employee, business associate, or other agent of OKSHINE authorized to perform services necessary for operating and maintaining OKSHINE.

1.3 "Advisory Committee" means the Oklahoma Office of Management and Enterprise Services Health Information Technology Advisory Board.

1.4 "Authorized User" means those members of Participant's Workforce (including employees, agents, contractors and any other persons having access to the OKSHINE by virtue of their relationship with Participant) who are individually authorized by Participant to have access to the OKSHINE to assist Participant with respect to the permitted uses as provided herein, and to whom Participant has assigned a unique identifier for access to the OKSHINE.

1.5 "Breach" means a breach as defined in 45 C.F.R §164.402.

1.6 "Break the Glass" means In an emergency, doctors and other clinicians can view a medical record if they meet these conditions:

- The clinician believes it is a medical emergency and have an immediate need for attention. Waiting for consent would delay treatment and that the delay could pose a risk to a patient's health and life.
- The practitioner believes that the medical history available via OKSHINE is necessary to provide the proper medical care.
- The patient has not previously denied consent to that particular practitioner.

1.7 "Confidential and Proprietary Information" means, proprietary or confidential materials or information of a Participant or OKSHINE in any medium or format that Participant or OKSHINE labels as such upon disclosure. Message Content and HIE Data is excluded from the definition of Confidential and Proprietary Information because other provisions of this Participation Agreement and the DURSA address the appropriate protections for Message Content and HIE Data. Notwithstanding any label to the contrary, Confidential and Proprietary Information does not include Message Content; any information which is or becomes known publicly through no fault of a Receiving Party; is learned of by a Receiving Party from a third party entitled to disclose it; is already known to a Receiving Party before receipt from a Participant as documented by Receiving Party's written records; or, is independently developed by Receiving Party without reference to, reliance on, or use of, Participant's Confidential and Proprietary Information.

1.8 "Data Use and Reciprocal Support Agreement (DURSA)" means the first restatement of the multiparty legal agreement that established a trust framework between the participants of the nationwide eHealth Exchange that was updated on August 13, 2019. The OKSHINE is a participant of the eHealth Exchange.

1.9 "Health Insurance Portability and Accountability Act of 1996 (HIPAA)" means the administrative simplification

provisions of the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH Act, the regulations promulgated thereunder, including the Privacy Rule and the Security Rule, and all future changes or amendments to HIPAA or the regulations promulgated thereunder.

1.10 "HIE Data" shall mean the clinical and demographic data submitted to, exchanged and stored by OKSHINE together with such other PHI or individually identifiable information as may be necessary or proper to achieve the purposes of OKSHINE.

1.11 "HITECH Act" means Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009), the regulations promulgated thereunder, and all future changes or amendments to the HITECH Act or the regulations promulgated thereunder.

1.12 "Information Blocking" means a practice by a health IT developer of certified health IT, health information network, health information exchange, or health care provider that, except as required by law or specified by the Secretary of Health and Human Services (HHS) as a reasonable and necessary activity, is likely to interfere with access, exchange, or use of electronic health information (EHI).

1.13 "Intellectual Property Rights" means patent rights, copyrights, trade secrets, and any other intellectual property rights recognized in any country or jurisdiction in the world.

1.14 "Participant" means an authorized organization (including but not limited to, healthcare provider, hospital, health plan, and state government) that has voluntarily agreed to enter into this Participation Agreement to access or use the OKSHINE. Participants in the Network include data recipients that will access data through OKSHINE and data suppliers that will provide data through OKSHINE.

1.15 "Participation Fees" means the fees set forth in Exhibit D for OKSHINE services.

1.16 "Protected Health Information (PHI)" has the meaning set forth in the HIPAA privacy rule, 45 C.F.R. § 160.103, and includes any other Individually Identifiable Health Information relating to the past, present, or future physical or mental health of an Individual; the provision of health care to the Individual; or the payment for health care that is maintained by any medium and transmitted by electronic media or in any other form or medium.

1.17 "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information while in transit via the OKSHINE, or while being stored within OKSHINE systems, or interference with OKSHINE operations.

1.18 "Services" means the type of data transactions facilitated through OKSHINE.

1.19 "Treatment, Payment and Healthcare Operations (TPO)" has the meaning as such terms are defined in the Privacy Rule at 45 CFR 164.501.

1.20 "Workforce" means employees, volunteers, trainees, contractors, subcontractors, and other persons or entities whose conduct, in the performance of work for a covered entity, is under the control of such entity, whether or not they are paid by the covered entity.

SECTION 2 - GRANT OF RIGHTS TO USE SERVICES

2.1 During the Term, OKSHINE grants to Participant and Participant accepts:

a) a non-exclusive, nontransferable (except as provided herein) right to access and use OKSHINE, and

b) a non-exclusive, nontransferable (except as provided herein), limited license to use OKSHINE software furnished by OKSHINE.

Such access and use is subject to Participant's compliance with all applicable laws and regulations, the terms and conditions set forth in this Participation Agreement and the OKSHINE Policies. Participant shall obtain no rights to OKSHINE except for the limited rights to use OKSHINE expressly granted by this Participation Agreement.

2.2 Participant shall not: (a) make OKSHINE or services, in whole or in part, available to any other person, entity or business other than as set forth in this Participation Agreement; (b) reverse engineer, decompile or disassemble the software as a service provided by OKSHINE, in whole or in part, or otherwise attempt to discover the source code to the software used in OKSHINE ; or (c) modify the OKSHINE or combine the OKSHINE with any other software or services not provided or approved by OKSHINE; or (d) modify any security procedures or security software of or for OKSHINE.

SECTION 3 – ACCESS TO OKSHINE

3.1 Subject to the terms of this Participation Agreement, OKSHINE authorizes Participant to access OKSHINE and to use the Services for the purposes of TPO and public health reporting as authorized or required by applicable law.

3.2 Participant agrees not to access OKSHINE or use the Services for any other purpose other than as set forth in Section 3.1 above. In particular:

(a) Participant shall not knowingly reproduce, publish or distribute content in connection with OKSHINE that infringes any third party's trademark, copyright, patent, trade secret, publicity, privacy or other personal or proprietary right;

(b) Participant shall be responsible for its own compliance, including Participant's Authorized User compliance, with all OKSHINE Policies, applicable laws, including laws related to interoperability, information blocking, maintenance of privacy, security, and confidentiality of patient and other health information and the prohibition on the use of telecommunications facilities to transmit illegal, obscene, threatening, libelous, harassing or offensive messages or otherwise unlawful material;

(c) Participant shall not knowingly: (i) abuse or misuse OKSHINE or the services, including gaining or attempting to gain unauthorized access to OKSHINE or altering or destroying information in OKSHINE , except in accordance with accepted practices; (ii) use OKSHINE or services in such a manner that interferes with other Authorized Users use of OKSHINE ; (iii) permit the introduction into OKSHINE of any program, routine, subroutine, or data that does or may disrupt or in any way impede the operation of the OKSHINE , or alter or destroy any data within it;

(d) Participant shall not use OKSHINE or Services for the purpose of exploiting the health data of other participants, including aggregating health data from other participants for exploitation by third

parties;

(e) Participant shall not use OKSHINE or the Services in violation of the established OKSHINE Policies or any applicable laws of the state or federal governments including, without limitation, the responsibility to remove treatment information from a federally funded substance use disorder treatment center unless written consent of the patient is obtained as required by 42 USC 290dd-2(b)(1) and 42 C.F.R. 2.31(a) and any amendments, or unless another exception under the law is met; and

(f) Subpoenas and Aggregation:

(i) Participant shall not use OKSHINE to create, produce or compile records or health data of other participants for the purpose of furnishing copies of aggregated records to third parties, except for purposes of the Participant's TPO to the extent such uses are permitted under HIPAA or other applicable federal or state law, or as is otherwise required by law;

(ii) If Participant is subpoenaed or otherwise ordered to use OKSHINE for the purpose of compiling the health data of other participants that are not already contained in Participant's records, Participant shall immediately notify OKSHINE so that OKSHINE, and such other participants or interested parties as it may determine, might have an opportunity to appear or intervene and protect their respective interests; and

(iii) Neither Participant nor OKSHINE shall be required to contest any such subpoena or order and shall not be required to incur any expense in connection with legal proceedings or processes, whether initiated by OKSHINE or any other interested party, with respect thereto.

3.3 Participant's Records.

(a) Participant shall be solely responsible for compliance with any applicable regulatory requirements related to the preservation, privacy and security of its own records, including, without limitation, data backup, disaster recovery, and emergency mode operation. Participant acknowledges that OKSHINE does not undertake to provide such services.

(b) Participant may access and use the electronic health information as permitted in this Participation Agreement and may merge relevant parts of such electronic health information into its own.

(c) Nothing in this Section 3 or elsewhere in this Participation Agreement is intended or shall be deemed to limit the Participant's use of its own patient information in any way.

3.4 Privacy and Security Safeguards.

(a) Participant and OKSHINE shall implement and maintain reasonable and appropriate administrative, physical and technical safeguards to protect the confidentiality, privacy, security, integrity and availability of electronic health information accessible through OKSHINE, to protect it against reasonably anticipated threats or hazards, and to prevent its use or disclosure otherwise than as permitted by this Participation Agreement or required by law. To that end, each Participant and OKSHINE shall:

(i) provide for appropriate identification and authentication of their Authorized Users and

Administrative Users, respectively;

(ii) provide appropriate access authorization;

(iii) guard against unauthorized access to or use of protected health information; and

(iv) provide appropriate security audit controls and documentation; and

Such safeguards shall comply with HIPAA, all applicable federal, state, and local requirements, and OKSHINE Policies.

(b) Participant and OKSHINE shall each maintain reasonable and appropriate security practices, in accordance with at least the minimum standards and guidelines in the OKSHINE Security Policies with regard to all personnel, systems, physical and administrative processes used by each party to transmit, store and process electronic health information through the use of OKSHINE. Participant and OKSHINE each shall be responsible for establishing and maintaining their respective security management procedures, security incident procedures, contingency plans, audit procedures, facility access controls, workstation use controls and security, device and media controls, authentication procedures, and security policies and procedures to protect electronic health information accessible through OKSHINE.

(c) Participant shall notify OKSHINE within five (5) days of Participant's receipt of any adverse audit findings related to Participant's participation in OKSHINE and the resolution of such findings. As required through the Business Associate Agreement (Exhibit C), Participant shall notify OKSHINE of any Security Incident relating to OKSHINE interface or connection of which Participant becomes aware, or any unauthorized use or disclosure of information within or obtained from OKSHINE within five (5) days and shall cooperate with OKSHINE in investigating the incident and shall take such action to mitigate any breach or suspected breach. OKSHINE shall notify Participant of any Security Incident relating to the Participant's shared PHI of which OKSHINE becomes aware, or any unauthorized use or disclosure of Participant's PHI within, or obtained from, OKSHINE of which OKSHINE becomes aware, within five (5) days of OKSHINE becoming aware of either the Security Incident or unauthorized use or disclosure of Participant's PHI, and shall cooperate with Participant in investigating the Security Incident and shall take such action to mitigate any breach or suspected breach.

(d) When Transacting Message Content over the nationwide eHealth Exchange through OKSHINE, Participant shall (i) comply with all Applicable Law; (ii) reasonably cooperate with OKSHINE on issues related to this Participation Agreement and with the eHealth Exchange DURSA; (iii) Transact Message Content only for permitted purposes as outlined in Restatement II of the DURSA (FINAL August 13, 2019); (iv) use Message Content received from another Participant in accordance with the terms and conditions of this Participation Agreement; (v) Participant agrees to the Adverse Security Event Notification requirements outlined in the Restatement II of the DURSA (Final August 13, 2019) and associated eHealth Exchange Performance and Service Specifications and the Operating Policies and Procedures; (vi) refrain from disclosing to any other person any passwords or other security measures issued to the Authorized User by OKSHINE or the Participant Account Administrator; and (vii) comply with the provisions outlined in Restatement II of the DURSA (FINAL August 13, 2019) and the eHealth Exchange Performance and Service Specifications and the Operating Policies and Procedures. These policies are available at the eHealth Exchange website: https://ehealthexchange.org/policies/

(e) Qualified Service Organization Agreement. If, through a Participant's use of OKSHINE, OKSHINE's performance of its responsibilities described in OKSHINE Policies causes OKSHINE to act as a "Qualified Service Organization" (as defined in 42 C.F.R. Part 2), the Participant and OKSHINE shall enter into a separate Qualified Service Organization Agreement. https://oklahoma.gov/ohca/okshine/resources.html

3.5 Authorized Use.

(a) OKSHINE authorizes Participant to access and use OKSHINE. Participant authorizes its Authorized Users and obtains a unique ID for each of its Authorized Users. Participant shall adopt and maintain reasonable security precautions for Participant's and its Authorized Users' IDs to prevent their disclosure to or use by unauthorized persons; OKSHINE shall do the same with respect to OKSHINE's Administrative Users. Each Authorized User shall have and use the Authorized User ID assigned to them.

(b) Participant may permit Participant's Authorized Users to access and use OKSHINE and the Services on behalf of Participant, subject to the terms of this Participation Agreement. Participant shall:

(i) Provide the appropriate level of access to OKSHINE based on the role or function of the Authorized User in Participant's Workforce;

(ii) Require that its Authorized Users agree to the same restrictions and conditions that apply to the Participant with respect to health information;

(iii) Train all Authorized Users regarding the privacy, security and confidentiality requirements of this Participation Agreement, the OKSHINE Policies, and applicable law relating to their access to and use of OKSHINE and the Services. Participant shall be responsible for their compliance with such requirements;

(iv) Take such disciplinary action as it may deem appropriate against any Authorized User who violates the confidentiality provisions of this Participation Agreement or OKSHINE Policies; and

(v) Notify OKSHINE within 24-hours of the termination, revocation or restriction of employment or right of access of any Authorized User (or if the individual is not an employee, of the termination of the relationship with Participant which granted the individual access to OKSHINE).

3.6 Termination of Participant Access. Following written notice to a Participant and a period of sixty (60) days to cure (if such cure is possible) OKSHINE may terminate the Participant's access to OKSHINE on a temporary or permanent basis for reasons including, without limitation, adverse audit findings related to Participant's or its Authorized Users' use of OKSHINE , breaches of the terms and conditions of this Participation Agreement or OKSHINE's Policies, default in payment of Participation Fees, HIPAA incidents, privacy or security breaches, or failure to take reasonable remedial action when a Breach is discovered, including, without limitation: (i) failure to cooperate in mitigating damages, (ii) failure to appropriately discipline an Authorized User or other person under the Participant's control for security or privacy violations, or (iii) other actions that undermine the confidence of other participants in the effectiveness of OKSHINE safeguards. When terminating access, OKSHINE shall explain to Participant the basis and shall provide support for its action. A permanent termination of access shall be followed

by termination of this Participation Agreement. If this Participation Agreement is terminated by OKSHINE pursuant to this subsection (3.6), Participant shall not be entitled to a refund of Participation Fees for the unexpired term. Participant acknowledges the duty to protect the confidentiality and security of PHI may extend beyond term of this agreement and the accompanied Business Associate Agreement (BAA).

3.7 Professional Responsibility. Participant or Authorized User shall be solely responsible for the medical, professional and technical services it provides. OKSHINE makes no representations concerning the completeness, accuracy or utility of any information in OKSHINE or concerning the qualifications or competence of individuals who placed it there. OKSHINE has no liability for the consequences to Participant, Authorized User or Participant's patients of Participant's use of OKSHINE or the Services.

3.8 Cooperation. OKSHINE Administrative Users and Participant Authorized Users shall cooperate with the reasonable audit and investigation of potential violations of law or the terms of this Participation Agreement, including but not limited to compliance investigations and privacy and security breaches.

SECTION 4 - INFORMATION AVAILABLE THROUGH OKSHINE

4.1 Accuracy and Format of Health Information. Participant shall use reasonable efforts to ensure that Participant's shared Information:

(a) Is current, accurate and (subject to any restrictions imposed by law or this Participation Agreement, including Section 3.2 (e)) complete; and

(b) Complies with any requirements of OKSHINE Policies as to format or content.

4.2 Use and Disclosure of Participant's shared Information.

(a) Participant authorizes OKSHINE to facilitate the exchange of Participant's shared Protected Health Information to other Participants for purposes of TPO and Public Health Activities, to the extent such exchange would be required or authorized by law if done by Participant.

(b) OKSHINE may use, maintain and disclose Participant's shared Protected Health Information to carry out OKSHINE's duties under OKSHINE policies, including without limitation, system administration, testing, problem identification and resolution, management of OKSHINE , facilitate Oklahoma Public Health Reporting, and data aggregation activities as permitted by applicable state and federal laws and regulations, including without limitation, those promulgated under HIPAA, and otherwise as OKSHINE determines is necessary and appropriate to comply with and carry out its obligations under all applicable federal, state and local laws and regulations.

4.3 Reliance on Representations. Participant acknowledges that in granting access to OKSHINE for the purposes as set forth in this Participation Agreement, OKSHINE will rely on the assurances of all other Participants as to (i) their identity and credentials, (ii) the purposes for which they are accessing OKSHINE , and (iii) the nature and extent of the information to which they will have access. Participant acknowledges that, while OKSHINE will contain certain technical safeguards against misuse of OKSHINE , it will rely to a substantial extent on the representations and undertakings of other Participants and their Authorized Users. Participant agrees that OKSHINE shall not be responsible for any unlawful access to or use of Participant's shared Protected Health Information by any other Participants resulting from misrepresentation to OKSHINE, breach of their participation agreements, or violation of OKSHINE Policies, unless such unlawful access to or use of Participant's shared

Information is due to OKSHINE's or its agent's gross negligence, recklessness, or willful misconduct or omission.

4.4 Individuals' Rights. Participant is solely responsible for ensuring that Participant's shared Information may properly be disclosed for the purposes set forth in this Participation Agreement. In particular, Participant shall:

(a) Obtain any necessary consents, authorizations or releases from individuals required by agreement or by law for making their health information available in OKSHINE, to include taking all necessary action in the event that consent, authorization or releases are revoked, expired or having other conditions; and

(b) Include such statements (if any) in Participant's Notice of Privacy Practices as may be required in connection with Participant's use of OKSHINE.

(c) OKSHINE and Participant shall be responsible for affording individuals their rights with respect to the individual's electronic health information as required in the HIPAA Privacy Rules, HITECH Act, and 21st Century Cures Act.

4.5 Rights to Health Information. If Participant Data has been used or disclosed for public health reporting, public health activities or TPO, it may thereafter be integrated into the records of the Participant.

SECTION 5 - ESTABLISHMENT OF OKSHINE POLICIES

5.1 Generally. OKSHINE Policies shall apply to the operation of OKSHINE, the services provided by OKSHINE, and the relationships among OKSHINE and Participants. OKSHINE and each Participant agrees to comply with OKSHINE Policies, which can be found at, h https://oklahoma.gov/ohca/okshine/resources.html applicable to the Participant, and, subject to the provisions of Section 5.2 of this Participation Agreement, with any amendments to OKSHINE Policies.

5.2 Amendment of OKSHINE Policies.

5.2.1 Procedures for Amendment of OKSHINE Policies. OKSHINE is solely responsible for the development of OKSHINE Policies, and may amend, or repeal and replace, OKSHINE Policies at any time as OKSHINE determines is appropriate. OKSHINE shall notify all Participants of any changes to OKSHINE Policies and Procedures at least thirty (30) days prior to the implementation of the change; provided that, if the change requires modifications to the Participant's system or may otherwise materially affect the Participant's operations or obligations under the Participation Agreement, OKSHINE shall notify the Participant at least sixty (60) days prior to the implementation of the change. Notwithstanding the foregoing, if the change is required in order for OKSHINE or the Participants to comply with applicable laws or regulations, OKSHINE may implement the change within a shorter period of time as OKSHINE reasonably determines is appropriate under the circumstances; provided that OKSHINE shall provide the Participants with as much notice of any such change as reasonably possible.

5.2.2 Any change to OKSHINE Policies shall automatically be incorporated by reference into this Participation Agreement and be legally binding upon OKSHINE and the Participant, as of the effective date of the change.

SECTION 6 - SOFTWARE AND HARDWARE

6.1 Description. Participant acknowledges that in order to access and use OKSHINE, it may be necessary for Participant to acquire, install, configure and maintain hardware, software and communication systems in order to connect to OKSHINE and comply with this Participation Agreement. The parties acknowledge that the Participant will be responsible for all costs associated with any modifications to its internal systems to enable its connection to OKSHINE. Participant acknowledges that amendments to the configuration of its systems and technical environment may impact the OKSHINE Services.

6.2 Open-Source Software. Nothing in OKSHINE Policies may be construed to limit any use of open-source software in accordance with the applicable open-source software license.

SECTION 7 - OTHER PARTICIPANT OBLIGATIONS

7.1 Indemnification. Participant is responsible for its own compliance with the terms of this Participation Agreement, HIPAA, the OKSHINE Policies, and all applicable laws and regulations. Participant shall be solely responsible for the use of OKSHINE by Participant and its workforce. Participant will defend, indemnify and hold OKSHINE, its officers, directors, agents, and employees, harmless against any and all claims, liabilities, damages, judgments or expenses (including attorneys' fees) asserted against, imposed upon or incurred by OKSHINE, that arise out of the willful misconduct or negligent acts or omissions of Participant or its employees, agents, or representative including claims brought by third parties arising out of Participant's use, or distribution, of any data obtained through the use of OKSHINE's services.

7.2 Other Resources.

a) Each Participant is responsible for providing such other resources as may be reasonably necessary in connection with the implementation of the OKSHINE, including making available such Participant staff members as may be necessary for these purposes.
b) Each Participant shall, at its own expense, utilizing the user manuals and other resources provided by OKSHINE, provide to all Authorized Users appropriate and adequate training regarding, without limitation, access to and use of OKSHINE Services, privacy and security of Patient Data obtained using the OKSHINE Services, and applicable OKSHINE policies.

SECTION 8 - OKSHINE'S OPERATIONS AND RESPONSIBILITIES

8.1 Execution of Participation Agreement. OKSHINE shall require that all Participants enter into a Participation Agreement and Business Associate Agreement, as applicable, prior to being granted access to and use of OKSHINE and Services.

8.2 Participant Training. OKSHINE shall provide training to each Participant regarding access and use of OKSHINE and Services, including such user manuals and other resources as OKSHINE determines appropriate so that the Participant may train all of its Authorized Users regarding access to and use of OKSHINE Services, privacy and security of Patient Data, and applicable OKSHINE Policies as required under Section 7.2 of this Participation Agreement.

8.3 Telephone and/or E-Mail Support. OKSHINE shall provide, directly or through a business associate or other agent, by telephone or e-mail, support and assistance in resolving technical issues in accessing and using OKSHINE and Services, in accordance with OKSHINE Policies.

8.4 Access Monitoring. Each party represents that, through its agents, employees and independent contractors, it shall have the ability to monitor and audit all access to and use of its System related to this Agreement, for system administration, security and other legitimate purposes. Each party shall perform those monitoring activities required by the OKSHINE Policies and Procedures.

8.5 Compliance with Laws and Regulations. Without limiting any other provision of this Participation Agreement and OKSHINE Policies relating to the parties' compliance with applicable laws and regulations, OKSHINE agrees to comply with applicable federal, state, and local laws relating to its operation of OKSHINE.

8.6 Viruses and Other Threats. OKSHINE shall use reasonable efforts to ensure that OKSHINE does not include, and will not introduce, any program, routine, subroutine, or data that will disrupt the proper operation of any hardware or software used by a Participant in connection with OKSHINE and Services.

8.7 Intellectual Property Rights. Subject to compliance by the Participant with the provisions of this Participation Agreement, OKSHINE warrants that it has all rights and licenses necessary to provide OKSHINE and Services to the Participant without violating any intellectual property rights of any third party.

SECTION 9 – PARTICIPATION FEES

9.1 Annual Participation Fees. In consideration for OKSHINE providing Participant with the Services, Participant agrees to pay the annual Participation Fees as adopted by the Advisory Committee and specified in Exhibit D. OKSHINE shall notify all Participants of its intent to modify fees in writing at least sixty (60) days prior to the implementation of the change.

9.2 Payment. The Participation Fees shall be due and payable to OKSHINE within thirty (30) days of invoice. Failure to pay the annual Participation Fees within such time shall constitute a material breach of this Participation Agreement.

9.3 Taxes. All charges and fees shall be exclusive of all federal, state, municipal, or other government excise, sales, use, occupational, or like taxes now in force or enacted in the future, and Participant agrees to pay any tax that OKSHINE may be required to collect or pay now or at any time in the future and that are imposed upon the sale or delivery of items and Services purchased under this Participation Agreement.

9.4 Other Fees. Participant is responsible for any charges Participant incurs to use OKSHINE, such as interface fees, network and equipment charges, and fees charged by Participant's third-party vendors of products and services.

SECTION 10 – CONFIDENTIAL AND PROPRIETARY INFORMATION

10.1 Scope of Confidential and Proprietary Information. In the performance of their respective responsibilities pursuant to this Participation Agreement, OKSHINE and Participants may come into possession of certain Confidential and Proprietary Information of the other party.

10.2 Nondisclosure of Confidential and Proprietary Information. OKSHINE and the Participant each (i) shall keep

and maintain the confidentiality of all Confidential and Proprietary Information received from the other, or from any of the other's employees, accountants, attorneys, consultants, or other agents and representatives, in connection with the performance of their respective obligations under this Participation Agreement; (ii) may not use, reproduce, distribute or disclose any such Confidential and Proprietary Information except as necessary to carry out its duties under this Participation Agreement or as required by law; and (iii) shall prevent its employees, accountants, attorneys, consultants, and other agents and representatives from making any such use, reproduction, distribution, or disclosure of Confidential and Proprietary Information, except in connection with the performance of their respective obligations under this Participation Agreement.

SECTION 11 - DISCLAIMERS, EXCLUSIONS OF WARRANTIES, LIMITATIONS OF LIABILITY

11.1 Carrier lines. Participant acknowledges that access to the OKSHINE is to be provided over various facilities and communications lines, and information may be transmitted over local exchange and internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and internet service providers, all of which are beyond OKSHINE's control. OKSHINE is not liable for any damages relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted on the carrier lines, or any delay, failure, interruption, interception, loss, transmission, or corruption of any data or other information attributable to transmission on the carrier lines. Use of the carrier lines is solely at the Participant's or Authorized User's risk and is subject to all applicable local, state, national, and international laws.

11.2 NO WARRANTIES. EXCEPT AS SET FORTH IN THIS SECTION, OKSHINE SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

THE PARTICIPANT IS SOLELY RESPONSIBLE FOR ANY AND ALL ACTS OR OMISSIONS TAKEN OR MADE IN RELIANCE ON OKSHINE OR THE INFORMATION IN THE SYSTEM, INCLUDING INACCURATE OR INCOMPLETE INFORMATION.

IT IS EXPRESSLY AGREED THAT IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING LOSS OF PROFITS OR REVENUES, LOSS OF USE, OR LOSS OF INFORMATION OR DATA, WHETHER A CLAIM FOR ANY SUCH LIABILITY OR DAMAGES IS PREMISED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER THEORIES OF LIABILITY, EVEN IF THE PARTY HAS BEEN APPRISED OF THE POSSIBILITY OR LIKELIHOOD OF THOSE DAMAGES OCCURRING.

EACH PARTY DISCLAIMS ANY AND ALL LIABILITY FOR ERRONEOUS TRANSMISSIONS AND LOSS OF SERVICE RESULTING FROM COMMUNICATION FAILURES BY TELECOMMUNICATION SERVICE PROVIDERS OR THE HOSTED SYSTEM.

NOTWITHSTANDING ANY OTHER PROVISION OF THIS PARTICIPATION AGREEMENT, OKSHINE'S TOTAL AND AGGREGATE LIABILITY TO A PARTICIPANT FOR ANY DAMAGES ARISING OUT OF, BASED ON, OR RELATING TO THIS PARTICIPATION AGREEMENT, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), WARRANTY, OR ANY OTHER LEGAL THEORY (AND NOT OTHERWISE DISCLAIMED), MAY NOT EXCEED THE AMOUNT OF FEES ACTUALLY PAID BY THE PARTICIPANT UNDER THIS PARTICIPATION AGREEMENT IN THE TWELVE (12) MONTH PERIOD PRECEDING THE ACTS OR OMISSIONS GIVING RISE TO THE CLAIM.

11.3 Other Participants. Participant acknowledges that other Participants have access to the OKSHINE and are receiving services. The other Participants have agreed to comply with OKSHINE Policies, concerning use of the information made available through OKSHINE; however, the actions of these other parties are beyond the control of OKSHINE. Accordingly, OKSHINE does not assume any liability for or relating to any impairment of the privacy, security, confidentiality, integrity, availability, or restricted use of any information on the system resulting from any Participant's actions or failures to act, except when OKSHINE has been notified in writing of such a participant's actions or failures to act and has failed to take action to prevent further noncompliance with KOKSHINE Policies by that Participant.

11.4 Unauthorized Access; Lost or Corrupt Data.

11.4.1. As between a Participant and OKSHINE, the Participant is solely responsible for validating the accuracy of all output and reports.

11.4.2. The Participant waives any claims against OKSHINE for damages occasioned by lost or corrupt data, incorrect reports, or incorrect data files resulting from programming error, operator error, equipment or software malfunction, security violations, use of third-party software, or any other cause unless such damages are caused by OKSHINE's or its agent's gross negligence, recklessness, or willful misconduct or omission.

11.4.3. OKSHINE is not responsible for the content of any information transmitted or received through OKSHINE's provision of the Services.

11.4.4. Without limiting any other provision of this Participation Agreement or limiting any provision of OKSHINE's Policies, OKSHINE has no responsibility for, or liability related to any unauthorized access to the Participant's transmission facilities or equipment by individuals or entities using OKSHINE or for unauthorized access to, or alteration, theft, or destruction of the Participant's data files, programs, procedures, or information through the OKSHINE, whether by accident, fraudulent means or devices, or any other method.

11.5 Inaccurate Data. All Patient Data to which access is made through OKSHINE originates initially from Participants and is subject to change arising from numerous factors, including without limitation, changes to patient health information made at the request of the patient, changes in the patient's health condition, the passage of time and other factors. OKSHINE does not monitor the specific content of data being transmitted. Without limiting any provision of any other section of this Participation Agreement or OKSHINE's Policies, OKSHINE has no responsibility for or liability related to the accuracy, content, currency, completeness, content or delivery of any data either provided or used by a Participant, except to the extent that any such liability is the direct result of OKSHINE's grossly negligent misconduct.

11.6 Patient Care. Participant is solely responsible for all decisions and actions taken or not taken by the Participant or the Participant's Authorized Users involving patient care, utilization management, and quality management for its patients resulting from or in any way related to the use of OKSHINE or the data made available by the Services. Participant waives any claims against OKSHINE, for any loss, damage, claim, or cost relating to or resulting from its own use or misuse of OKSHINE or the data made available by the Services related to patient care, utilization management, and quality management for its patients.

11.7 Liability of Other Parties. Nothing in this Section may be construed as a limitation on any claims by OKSHINE or any Participant against a telecommunications carrier or other third-party vendor.

SECTION 12 - INSURANCE

12.1 Insurance. Participant agrees to obtain and maintain in full force and effect during the Term of this Participation Agreement insurance or self-insurance, including cybersecurity coverage, to insure itself and its Workforce, authorized users, agents, and contractors for liability arising out of activities to be performed under, or in any manner related to, this Participation Agreement. Such policy or policies shall be provided within ten (10) business days of written request by OKSHINE.

SECTION 13 - TERMINATION

13.1 Termination without Cause. Either party may terminate this Participation Agreement without cause upon sixty (60) days prior written notice to the other party.

13.2 Termination for Cause. OKSHINE shall have the right to terminate this Participation Agreement for cause as provided in Section 3.6 of this Participation Agreement. The Participant shall have the right to terminate this Participation Agreement in the event of a material breach of this Participation Agreement by OKSHINE which is not cured within sixty (60) days of delivery of written notice of the breach; provided that, if the breach is capable of cure but not within sixty (60) days, this Participation Agreement shall not be terminated as long as OKSHINE commences to cure the breach within sixty (60) days, provides appropriate notice to participant, and diligently pursues the cure to completion.

13.3 Effect of Termination. Upon any termination of this Participation Agreement with respect to a Participant, neither the Participant nor its Authorized Users have any rights to use OKSHINE and neither OKSHINE nor any of the other Participants may have any further access to Patient Data of that Participant through OKSHINE. This section does not apply to the duty of a Participant that ceases operations to store, make arrangements to store, or make available to patients the Participant's Patient Data which is subject to other law.

13.4 Survival Provisions. Any provision of this Participation Agreement that contemplates or requires performance subsequent to any termination of this Participation Agreement survives any termination of the Participation Agreement, including, but not limited to, Section(s) 3.4, 10,11 and this Section.

SECTION 14 - GENERAL PROVISIONS

14.1 Applicable Law. This Participation Agreement shall be governed by the laws of Oklahoma, without reference to the principles of Oklahoma law respecting conflicts of laws. Any action or other proceeding arising under or in connection with this Participation Agreement, must be adjudicated exclusively in an Oklahoma District Court or a federal court in Oklahoma.

14.2 Assignability. The rights of OHCA under this Participation Agreement may be assigned or transferred to a State designated non-profit 501(C)(3) organization charged with facilitating the exchange of health information to and from authorized individuals and healthcare organizations in this state. No other rights of either party under this Participation Agreement may be assigned or transferred by a party, either voluntarily or by operation of law, without the prior written consent of the other party, which that party may withhold in its sole discretion.

14.3 Supervening Circumstances. Neither the Participant nor OKSHINE may be considered in violation of any

provision of this Participation Agreement if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other natural occurrences, including health pandemics; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other civil or military emergencies; (f) acts of legislative, judicial, executive, or administrative authorities; or (g) any other circumstances that are not within its reasonable control other than a lack of financial resources. This Section does not apply to obligations imposed under applicable laws and regulations.

14.4 Severability. Any provision of this Participation Agreement or OKSHINE Policies that proves to be invalid, void, or illegal, shall in no way affect, impair, or invalidate any other provision of this Participation Agreement and OKSHINE Policies, and all such other provisions shall remain in full force and effect.

14.5 Notices. Any and all notices required or permitted under this Participation Agreement shall be considered to have been properly given when delivered if delivered in person; upon receipt if mailed by first class mail, postage, prepaid; within five (5) business days if mailed by certified or registered mail, return receipt requested; or within one (1) business day if delivered by commercial courier that can confirm delivery, and when addressed to the parties as specified in Exhibit B, or as the parties may otherwise specify in accordance with this provision.

14.6 Waiver. No provision of this Participation Agreement shall be considered waived and no breach excused, unless the waiver or consent is in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of a breach by the other, whether expressed or implied, does not constitute a consent to, waiver of, or excuse for any other different or subsequent breach.

14.7 Injunctive Relief. Each of the parties acknowledges and agrees that nothing in this Participation Agreement shall interfere with any right of the other party or the other Participants to injunctive or other equitable relief.

14.8 Third Party Beneficiaries. Except as expressly provided in Section 14.7 (with respect to injunctive relief), there are no third-party beneficiaries of this Participation Agreement.

14.9 Complete Understanding. This Participation Agreement, together with the Business Associate Agreement and any exhibits in effect between the parties and OKSHINE Policies, contains the entire understanding of the parties to this Participation Agreement, and there are no other written or oral understandings or promises between the parties with respect to the subject matter of this Participation Agreement other than those contained or referenced in the Participation Agreement. All amendments to this Participation Agreement shall be in writing and signed by all parties.

14.10 Publicity. No public announcements, media releases, press conferences, advertising or similar publicity in any form relating to the name, image, or logo of either party or any of its affiliates shall be made without the prior written consent of the other party, except as required for operation of the OKSHINE, as for example, for publishing a list of Participants or as otherwise contemplated by this Agreement or as required by Applicable Law. The limitations set forth in this Section do not apply to any documents that either party may be required to provide to a federal, state, or local governmental agency.

14.11 Independent Contractors. The parties to this Participation Agreement are separate and independent entities. Nothing in this Participation Agreement may be construed or be considered to create a relationship of employer and employee, principal and agent, partnership, joint venture, or any relationship other than that of independent entities who have entered into this Participation Agreement solely for the purposes provided.

14.12 Counterparts. The parties may execute this Participation Agreement in counterparts, each of which is considered an original and all of which only constitute one original.

SECTION 15 - CREATING, USING, AND DISCLOSING PHI FOR RESEARCH

15.1 Review of Research Requests.

(a) OKSHINE, from time to time, may act as Participants' Business Associate for purposes of reviewing requests for the use and disclosure of data submitted to OKSHINE for research purposes. When OKSHINE reviews a research proposal or project for the use of PHI, OKSHINE will verify the identity of the person or entity requesting the PHI and also verify the authority under which the request for PHI is made.

(b) Any research proposal that OKSHINE reviews that proposes to use all or any subset of the PHI must contain at least: (a) the name(s) of the sponsor(s) of the research and the name(s) of any institution(s) under whose auspices the sponsor(s) is working; (b) the specific question to be addressed by the research (no researcher shall be permitted to access the PHI without identifying a targeted goal for the research); (c) the PHI to which access is requested; (d) the proposed use of said PHI; (e) whether the research will require the identification of specific patients; (f) whether the research will require the identification of specific Participants; (g) any proposed publication of the results of the research; and (h) the means for protecting the confidentiality of the PHI.

(c) OKSHINE shall require third parties to warrant that research publications arising from the use of PHI under this Section 15 will contain only aggregate data and will not directly or indirectly identify any patient whose PHI is received pursuant to this Agreement unless a specific authorization to do so is obtained from a patient.

(d) In no event will OKSHINE allow PHI to be disclosed for research projects that have the effect of comparing the Participants (such as individual Participant outcomes, Participant financial information, or charges to patients or third-party payors and similar reimbursement data) without specific written approval from each of the institutions involved or unless such comparisons are an implicit component of a research project that complies with the provisions of Section 9.2(a).

15.2 Research By OKSHINE or Third Parties:

(a) *General Rule - Approvals Required.* Except as otherwise provided below in this Section 9.2, any use or disclosure of the PHI (whether in identified or de-identified form) for research shall be proposed to OKSHINE and approved by: (1) an Institutional Review Board designated or approved by OKSHINE and (2) the Research Subcommittee (except as provided below). Prior to allowing the use of PHI of a Participant supplied to OKSHINE for research purposes, a Participant may require that the project be subjected to the review of an Institutional Review Board of its own choice. A Participant may decline to allow PHI it supplied to be used for a particular study, but that shall not preclude the use or disclosure of the remaining Participants' submitted PHI for such project. At the request of the Governing Body, the Research Subcommittee shall provide reports of the research disclosures approved by the Research Subcommittee pursuant to this Section; however, the reports provided by the Research Subcommittee to the Governing Body are for informational purposes only. The Parties agree that PHI may be used and disclosed, consistent with the appropriate Institutional Review Board approval, after approval by the Research Subcommittee which shall be organized and administered as follows:

(1) Each Participant will be entitled to be represented by an individual on the Research Subcommittee. Each Participant shall specifically identify the individual it desires to represent it on the Research Subcommittee and this individual shall be known as the Participant's Designated Research Representative. Such Designated Research Representative shall have full authority to act on behalf of the Participant with regard to duties assigned to the Research Subcommittee. OKSHINE shall also be represented by an individual to serve on the Research Subcommittee. All research proposals or requests shall be provided to the Research Subcommittee and voted on by the Designated Research Representatives. The Research Subcommittee will meet or confer from time to time, in person or electronically (at its discretion), to consider and render a decision as to any research proposals presented to OKSHINE. OKSHINE shall be able to fully rely on the actions and representations of a Participant's Designated Research Representatives or any proxy representative that the Participant chooses to send to a meeting or communicate with OKSHINE, and shall be fully

protected in such reliance.

(2) Each Participant and OKSHINE shall be entitled to exercise one vote through its Designated Research Representative on decisions made by the Research Subcommittee. In the event that the Research Subcommittee is unable to unanimously approve a research proposal, the research proposal shall be proposed to the Governing Body and approved by the Governing Body; provided, however, that only Participants whose submitted PHI will be used in the research proposal shall be entitled to cast a vote and any relevant quorum or majority voting requirements set forth in this Agreement shall be reduced proportionately.

(b) *No Further Approvals Required - Independent Agreements Between Participants and OKSHINE.* If OKSHINE has entered into, or enters into, any other agreement with one or more Participants that complies with the HIPAA with regard to the research uses and disclosures of the Participant's own PHI stored in OKSHINE, the provisions of such an agreement shall govern the use and disclosure of that Participant's PHI and the approvals required by Section 15.2(a) shall not be required.

(c) *No Further Approvals Required - Preparatory to Research and Decedents' Research.* OKSHINE (as Participants' Business Associate) may, and the Participants (as Covered Entities) hereby delegate the authority to OKSHINE to, authorize the use or disclosure of PHI (whether in identified or de-identified form) for research projects without further approval from Participants under Section 9.2(a), if the research projects meet the following criteria (provided that all HIPAA requirements regarding research have been met, including, but not limited to, the guidelines set forth in Section 15.3):

(1) OKSHINE may use or disclose identifiable PHI for reviews preparatory to research (consistent with 45 CFR § 164.512(i)(1)(ii); and

(2) OKSHINE may use and disclose identifiable PHI for research on decedent's information (consistent with 45 CFR § 164.512 (i)(l)(iii).

OKSHINE reserves the right to require a waiver of authorization from an Institutional Review Board acceptable to OKSHINE. At the request of a Participant, OKSHINE shall provide reports of the research disclosures made pursuant to this Section.

(d) *No Further Approvals Required - Certain Disclosures of De-identified Information and Limited Data Sets.* OKSHINE (as Participants' Business Associate) may, and the Participants (as Covered Entities) hereby delegate the authority to OKSHINE to, authorize the use or disclosure of PHI that has been de-identified in accordance with HIPAA or Limited Data Sets to any entity that has obtained an approval from an Institutional Review Board acceptable to OKSHINE for the use of PHI that has been de-identified in accordance with HIPAA or Limited Data Sets in connection with a research project. Further, OKSHINE may use or disclose PHI that has been de-identified in accordance with HIPAA or Limited Data Sets without further approval from a Participant if such PHI that has been de-identified in accordance with HIPAA or Limited Data Sets are included in classes or categories of queries that are approved by the Governing Body or an Institutional Review Board acceptable to OKSHINE. At the request of a Participant, OKSHINE shall provide reports of the research disclosures made pursuant to this Section.

15.3 Guidelines for Using and Disclosing PHI: When a research project has been approved pursuant to Section 9.2, OKSHINE shall act as the Participants' Business Associate for purposes of disclosing the PHI to the researchers. OKSHINE shall use the following guidelines when using or disclosing PHI or de-identified data:

(a) *Initial Determination of Scope of PHI To Be Disclosed.* For each research project, OKSHINE shall make a threshold determination of whether the minimum necessary use or disclosure of PHI to comply with the request involves the use or disclosure of identifiable PHI, a Limited Data Set, or PHI that has been de-identified in accordance with HIPAA. In making this threshold determination and when further disclosing PHI in connection with the research project, OKSHINE may rely on and adopt the determination of an Institutional Review Board as to the scope of the minimum necessary disclosure for the research project. If a research disclosure is made pursuant to an Individual's authorization, the scope of the authorization shall constitute the minimum necessary disclosure. In the event OKSHINE determines it is necessary to disclose the entire subset of PHI on the Network concerning an Individual to comply with the research request, OKSHINE will document the justification for releasing the entire subset of PHI. An Institutional Review Board's determination that the entire subset of PHI on the Network

is necessary, or an Individual's authorization, shall constitute such documentation.

(b) *Conditions For Disclosing Individually Identifiable Health Information.* If PHI is requested for a research project, OKSHINE shall not use or disclose the PHI unless: *(A)* authorizations that comply with the HIPAA allowing the use or disclosure of the PHI for the specific research purpose are obtained or have obtained from all Individuals whose Information will be used or disclosed; or (B) a waiver of the authorization is obtained from an appropriate Institutional Review Board or Privacy Board in accordance with 45 CFR § 164.512(i). Notwithstanding the foregoing, OKSHINE may use or disclose identifiable PHI for reviews preparatory to research (consistent with 45 CFR § 164.512(i)(1)(ii) and for research on decedent's information (consistent with 45 CFR § 164.512 (i)(1)(iii) without an authorization or the waiver thereof; provided that the use or disclosure of the PHI is consistent with the minimum necessary standard of the HIPAA. This Section 9.4(b) shall not apply to information in a Limited Data Set or de-identified information.

(c) *Conditions For Disclosing Limited Data Sets.* If a Limited Data Set is requested for a research project, OKSHINE shall not use or disclose the PHI unless OKSHINE, on behalf of the affected Covered Entity Participants, obtains a "Data Use Agreement" from the individual or entity using the Limited Data Set or to which the Limited Data Set will be disclosed, which is acceptable to the Covered Entity Participants. Such Data Use Agreement shall comply with the requirements of 45 CFR § 164.514(e). OKSHINE further agrees to maintain copies of all Data Use Agreements related to Covered Entity Participants' submitted PHI and to forward same to the Covered Entity upon request.

(d) *Conditions For Disclosing PHI that Has Been De-Identified.* If PHI that has been de-identified in compliance with HIPAA is to be used or disclosed, OKSHINE shall act as Covered Entities' Business Associate for purposes of de-identifying the PHI and shall ensure that no health data that is used or disclosed identifies an Individual and that there is no reasonable basis to believe that the de-identified information can be used to identify an Individual. All de-identification of PHI shall be conducted in compliance with 45 CFR § 164.514(a)-(c).

15.4 Involvement of Participant Investigator in Research: As a condition of approval of a research project not conducted by OKSHINE, any sponsor of research using all or any subset of the PHI shall be required to invite an investigator from any Participant whose PHI is used in the research and an investigator from OKSHINE to participate in the research project.

15.5 Access to Network by Researchers: No researcher, other than OKSHINE, shall have direct access to PHI on the Network (although access to de-identified information and Limited Data Sets may be permitted if allowed under Section 9.2 and 9.3). PHI that is requested by researchers other than OKSHINE shall be retrieved by representatives of OKSHINE. Any use of the PHI for research by OKSHINE shall be limited to the purpose of the research as approved or allowed by Section 9.2.

15.6 Cooperation by Participants' in Network Evaluations: The Participants agree to cooperate in studies conducted from time to time by the OKSHINE related to various issues surrounding the Network, including, but not limited to, the efficacy and usefulness of the Network. Such cooperation by the Participants may include, but not be limited to, participation in interviews, the completion of surveys, and the submission of other written or oral evaluations.

EXHIBIT B - PRIMARY CONTACTS AND ADDRESS FOR NOTICE

Addresses for Notice: Participant is required to provide information in the Contact fields below.

Participant Primary Contact

Name: _____

Title: _____

Organization: _____

Address: _____

City, State, Zip Code: _____

Organization Phone: _____

OKSHINE Address for Notice

OKSHINE
c/o Oklahoma Health Care Authority
4345 N Lincoln Blvd
Oklahoma City, OK 73105

Other Participant Contacts

Billing Contact:_____Email: _____

Phone: _____

If different than Primary **(All invoices are sent via e-mail)**

Technical Contact_____Email: _____

Phone: _____

Privacy Officer_____Email: _____

Phone: _____

Security Officer(If different than Privacy Officer)_____Email:_____

Phone:_____

EXHIBIT C – BUSINESS ASSOCIATE AGREEMENT (BAA)

RECITALS

WHEREAS, the Parties hereby enter into this BAA whereby Business Associate will provide certain services to Covered Entity; and

WHEREAS, pursuant to this BAA, Covered Entity wishes to disclose certain information to Business Associate, some of which may constitute Protected Health Information ("PHI") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), located at 42 U.S.C. 1320d-3120d-9, and its implementing regulations at 45 CFR 160 and 45 CFR 164 ("HIPAA Security and Privacy Rule"), the Health Information Technology for Economic and Clinical Health Act of 2009 (P.L. 111-5) (the "HITECH Act"), and with other applicable laws; and

WHEREAS, it is the goal of the Parties to protect the privacy and provide for the security of PHI owned by Covered Entity that is disclosed to Business Associate or accessed, received, stored, maintained, modified, or retained by Business Associate in compliance with HIPAA, the HITECH Act, and the HIPAA Security and Privacy Rule; and

WHEREAS, the purpose and goal of this BAA is to satisfy certain standards and requirements of HIPAA, HITECH Act, and the HIPAA Security and Privacy Rule, including but not limited to 45 CFR 164.502(e) and 45 CFR 164 504(e), as may be amended from time to time;

THEREFORE, in consideration of mutual promises made between the Parties and the exchange of information pursuant to this BAA, Covered Entity and Business Associate agree as follows:

A.1 PURPOSE

The purpose of this BAA is described in the Recitals above, and is more particularly described in Section B.

A.2 THE PARTIES

1. Oklahoma Health Care Authority (OHCA) d.b.a. the Oklahoma State Health Information Network and Exchange ("OKSHINE" or "Business Associate")
    a. OKSHINE has authority to enter into this BAA pursuant to 63 O.S. § 5006(A), 74 O.S. § 85.1 *et. seq.* OHCA's Chief Executive Officer has authority to execute this BAA on OHCA's behalf pursuant to 63 O.S. § 5008(B).
    b. OKSHINE's mailing address for the purposes of this BAA is as follows:

        OKSHINE
        c/o Oklahoma Health Care Authority
        Attn: Contracts Development Unit
        4345 N. Lincoln Boulevard
        Oklahoma City, OK 73105-5101

2. Covered Entity
    a. Covered Entity mailing address and contact information for the purposes of this BAA is included in Section B.

A.3 GENERAL PROVISIONS

1. Amendments**/**Modifications
   This BAA contains all of the agreements of the parties and no oral representations by either party are binding. Any amendments and/or modifications to this BAA shall be in writing and signed by both parties.

2. Services Substitutions

Substitutions are not permitted without the written permission of Covered Entity or as authorized in the scope of work.

3. Public Disclosure
   Business Associate shall not cause public disclosures or news releases pertaining to this BAA without prior written approval of Covered Entity.

A.4 PAYMENTS AND REIMBURSEMENT

No payment shall be made under this BAA.

A.5 TERM AND TERMINATION

1. This BAA shall be effective upon the last date of signature and shall continue for the term stated in Section B, Paragraph B.2 (Agreement Term) or until terminated by either party, whichever is earlier.

2. Either party may terminate this BAA in whole or in part for cause with a thirty (30) day written notice to the other party. Either party may terminate this BAA in whole or in part without cause with a sixty (60) day written notice to the other party. All notices of termination under this paragraph shall be in writing.

3. Covered Entity may terminate this BAA immediately, in whole or in part, with a written notice to the Business Associate(s) when one of the following applies:
   a. If Covered Entity determines that Business Associate has violated any material term of this BAA;
   b. If Covered Entity determines that an administrative error occurred prior to performance; or
   c. Both parties agree to terminate immediately without cause.

4. Upon termination of this BAA, Covered Entity may require Business Associate to destroy or return all PHI received from or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form and retain no copies of such information, or if such return or destruction is not feasible, Business Associate will extend the protections of this BAA to the information and limit further Uses and Disclosures to those purposes that make the return or destruction of the information not feasible. If requested by Covered Entity upon termination, Business Associate will require that all originals and copies of PHI, on all media and as held by either Business Associate or its agents or subcontractors, will be either returned to Covered Entity or destroyed within twenty (20) business days of termination of this BAA and will certify on oath in writing to such return or destruction within such twenty (20) business days.

A.6 CONFIDENTIALITY AND SECURITY OF PROTECTED HEALTH INFORMATION

1. To the extent any provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including but not limited to the Privacy Rule and Security Rule, or the Health Information Technology for Economic and Clinical Health Act (HITECH) and its implementing regulations apply to this BAA, both parties agree to these terms. Business Associate acknowledges that in its role as Business Associate, it may have or obtain access to protected health information ("PHI"), including but not limited to individually identifiable health information, some of which may be Electronic Protected Health Information ("Electronic PHI" or "ePHI"), both as defined by HIPAA, and collectively referred to as "PHI."

2. Business Associate acknowledges and agrees that all PHI that is created or received by Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display by Covered Entity or its operating units to Business Associate or is created or received by Business Associate on Covered Entity's behalf shall be subject to this BAA, and further, to the extent Business Associate is acting as a Business Associate of Covered Entity pursuant to this BAA, the provisions herein shall apply and Business Associate shall be subject to the penalty provisions as specified in 45 CFR Part 160 as applicable to Business Associate.

3. Definitions:
   a. General: The following terms used in this BAA shall have the same meaning as those terms in HIPAA, the HITECH Act, and the Privacy and Security Rule: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by

Law, Secretary, Security Incident, Subcontractor, Protected Health Information, Unsecured Protected Health Information, and Use. Should there be any conflict between the mandatory provisions of HIPAA, the HITECH Act, or the HIPAA Security and Privacy Rule, and the provisions of this BAA, the mandatory provisions of HIPAA, the HITECH Act, or the HIPAA Security and Privacy Rule shall control. Where the provisions of this BAA differ from those mandated by HIPAA, the HITECH Act, or the HIPAA Security and Privacy Rule but are nonetheless permitted by HIPAA, the HITECH Act, or the Privacy and Security Rule, the provisions of this BAA shall control.

b. Business Associate shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. § 160.103, and in reference to the party to this BAA, shall mean the OKSHINE.
c. Covered Entity shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. § 160.103, and in reference to the party to this BAA, shall mean the entity whose name appears in Section B.
d. Discovery shall generally mean the first day a Security Incident or breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate.
e. HIPAA shall mean the Health Insurance Portability and Accountability Act of 1996 and the Privacy, Security, Breach Notification, and Enforcement Rules per 45 C.F.R. Part 160 and Part 164, all as may be amended, and related regulations, including Administrative Simplification rules at 42 U.S.C § 1320d et seq. and the HITECH Act of 2009.
f. HIPAA Security and Privacy Rule shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

4. Obligations of Business Associate:
    a. Business Associate may use PHI solely to perform its duties and responsibilities pursuant to this BAA. Business Associate acknowledges and agrees that PHI is confidential and shall not be used or further disclosed, in whole or in part, except as provided in this BAA, or as Required by Law. Specifically, Business Associate agrees it will and will require its employees, agents, vendors, and subcontractors to:
        i. Use or further disclose PHI only as permitted in this BAA or as Required by Law, including, but not limited to HIPAA.
        ii. Ensure that patient information is confidential and is not to be released pursuant to 42 U.S.C §1396a(a)(7), 42 C.F.R. §§ 431.300-431.306 and 63 O.S. § 5018. Business Associate agrees not to release the information governed by these requirements to any other person or entity without the approval of Covered Entity, or as required by law or court order.
        iii. Ensure that patient and provider information cannot be re-marketed, summarized except to the extent contemplated by this BAA, distributed, or sold to any other organization without the express written approval of Covered Entity.
        iv. Implement and document appropriate technical, physical, and administrative safeguards and comply with 45 C.F.R. Part 164 with respect to electronic PHI to prevent use or disclosure of PHI other than as provided for by this BAA, and to protect the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits for or on behalf of Covered Entity in accordance with HIPAA including but not limited to training all employees, agents, and subcontractors in HIPAA to protect Covered Entity's PHI and prevent, detect, contain, and correct Security violations in accordance with HIPAA; applying security patches and performing vulnerability assessments on a regular basis, and using encryption for all electronic transmission of PHI including forced TLS connections for email.
        v. Not use or disclose or otherwise make available Covered Entity's PHI to any entity or individual who is not subject to the laws of the United States.
        vi. Not receive remuneration from a third party in exchange for disclosing PHI received from or on behalf of Covered Entity.
        vii. Report to Covered Entity any use or disclosure of PHI that is not permitted under this BAA as soon as reasonably practicable upon discovery but not later than five (5) calendar days from discovery, and mitigate, to the extent practicable and in cooperation with Covered Entity, any harmful effects known to him/her/it in connection with a use or disclosure made in violation of this BAA.
        viii. Report potential known violations of 21 O.S. § 1953 to Covered Entity's Legal Division without delay, and in no event later than five (5) calendar days after discovery of an unauthorized act. In general, this criminal

statute makes it a crime to willfully and without authorization gain access to, alter, modify, disrupt, or threaten a computer system.

ix. Report to Covered Entity any security incident upon discovery within five (5) calendar days of knowledge of the incident, as defined in the Security Rule, with respect to electronic PHI, as well as any breaches of unsecured PHI as required by 45 C.F.R. § 164.400 *et seq*. A Security Incident shall include, but is not limited to, unwanted disruption or denial of service, unauthorized use of a system for processing or storing ePHI, or changes to system hardware, firmware, or software without Business Associate's consent. Reports shall solely include successful Security Incidents.

x. With the exception of law enforcement delays that satisfy the requirements of 45 C.F.R. § 164.412, notify Covered Entity promptly, in writing and without unreasonable delay and in no case later than five (5) calendar days, upon the discovery of a breach of unsecured PHI as reasonable in the HITECH Act or accompanying regulations, pursuant to the terms of 45 C.F.R. § 164.410. Such notice shall include, to the extent possible, the name of each individual whose unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such breach. Business Associate shall also, to the extent possible, furnish Covered Entity with any other available information that Covered Entity is required to include in any notification to individuals under 45 C.F.R. § 164.404(c) at the time of Business Associate's notification to Covered Entity or promptly thereafter as such information becomes available. Business Associate shall reasonably cooperate in Covered Entity's breach analysis procedures, including risk assessment, if requested, at no additional cost or expense to Covered Entity when the breach is due to the acts or omissions of Business Associate, its contractors, agents, employees, or vendors.

xi. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2) and 164.314(a)2)(I)(B), if applicable, ensure that any subcontractors, vendors, and agents to whom he/she/it provides PHI or who create, receive, use, disclose, maintain, transmit, or have access to Covered Entity's PHI agree to the same restrictions, conditions, and requirements that apply to the Business Associate under this BAA, including but not limited to implementing reasonable and appropriate safeguards to protect PHI and complying with the requirements of 45 C.F.R. Subpart C, by entering into a contract or other arrangement that complies with 45 C.F.R. § 164.504 and §164.314.

xii. Business Associate will make any amendment(s) to PHI in a designated record set as directed or agreed to by Covered Entity pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526.

xiii. Any disclosure of Covered Entity's data shall be approved in advance by Covered Entity and then only to individuals expressly authorized to review such information under applicable Federal or State laws. If Business Associate, employees, or subcontractors disclose(s) or attempt(s) to disclose Covered Entity data, an injunction may be sought to prevent that disclosure as well as any other remedies of law that may be available. Business Associate shall provide written notice to Covered Entity of any use or disclosure of PHI not provided for by this BAA of which Business Associate becomes aware within five (5) calendar days of its discovery.

xiv. Notwithstanding anything to the contrary herein, Business Associate shall promptly provide written notice to Covered Entity upon receipt of a subpoena or other legal process that seeks disclosure of Covered Entity data, unless precluded by law from providing notice, so that Covered Entity may have the opportunity to seek a protective order or other means of limiting or preventing disclosure, on its own behalf, with respect to such data. Business Associate will, to the extent allowed by law, fully cooperate with any attempt by Covered Entity to seek such a protective order, including but not limited to, when permitted by applicable law, withholding from production any data before Covered Entity has had a reasonable opportunity to seek such an order or to seek review of the denial of such an order or the issuance of an order that OHCA deems insufficiently protective.

xv. Business Associate will maintain and make available the information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR. § 164.528. As such, if Business Associate maintains a designated record set in an electronic format on behalf of Covered Entity, then Business Associate agrees that within thirty (30) days of Covered Entity's written request, Business Associate shall provide to Covered Entity a complete report of all disclosures from the designated record set

covering the six (6) years immediately preceding the date on which the accounting is requested. The report shall include all required content pursuant to 45 CFR § 164.528.

xvi. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under 45 C.F.R. Part 164, Subpart E comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s).

xvii. Business Associate will make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate, on behalf of the Covered Entity available to the Secretary for purposes of determining compliance with 45 C.F.R. Subpart E and other applicable rules or regulations.

xviii. To the extent allowed by law, Business Associate shall indemnify and hold Covered Entity harmless from all claims, liabilities, costs, and damages arising out of or in any manner related to the unauthorized use or disclosure of PHI or related to a Breach or violation of confidentiality obligations by Business Associate, its employees, subcontractors, vendors, or agents.

xix. Provide access in a timely manner to PHI maintained by Business Associate in a designated record set to Covered Entity, or if directed by Covered Entity, to an Individual in order to meet the requirements of 45 C.F.R. § 164.524. In the event that any Individual requests access to PHI directly from Business Associate, Business Associate shall promptly forward such request to Covered Entity. Any denials of access to the PHI requested shall be the responsibility of Covered Entity.

xx. Make PHI available in a timely manner to Covered Entity for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526.

xxi. Document disclosure of PHI and information related to such disclosure as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI, in accordance with 45 C.F.R. § 164.528, and within five (5) calendar days of receiving a request from Covered Entity, make such disclosure documentation and information available to Covered Entity. In the event the request for an accounting is delivered directly to Business Associate, Business Associate shall promptly forward such request to Covered Entity.

xxii. Make its internal policies, procedures, practices, books, and records related to the use and disclosure of PHI received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary of HHS, authorized governmental officials, and Covered Entity for the purpose of determining Business Associate's compliance with HIPAA. Business Associate shall give Covered Entity advance written notice of requests from DHHS or government officials and provide Covered Entity with a copy of all documents he/she/it makes available.

xxiii. Respond to Covered Entity's request for confirmation and certification of Business Associate's ongoing compliance with HIPAA, including but not limited to conducting regular security audits and assessments as necessary to evaluate its Security and Privacy practices.

5. Permitted Uses by Business Associate:

In addition to permitted uses under this BAA, Business Associate may use or disclose PHI as described below, only if such use or disclosure of PHI would not violate HIPAA and related rules and regulations if performed by Covered Entity:

i. Use PHI to de-identify the information in accordance with 45 C.F.R. § 164.514(a)-(c).

ii. Use or disclose PHI for its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that (i) the disclosure is required by law; or (ii) Business Associate obtains reasonable assurances from any person to whom the PHI is disclosed that such PHI will be kept confidential and will be used or further disclosed only as required by law or for the purpose(s) for which it was disclosed to the person, and the person commits to notifying Business Associate of any instances of which he/she/it is aware in which the confidentiality of the PHI has been breached;

6. Covered Entity Obligations:

a. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices in accordance with 45 C.F.R. §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

b. Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

c. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, or as mandated pursuant to Section 13405(c) of the HITECH Act, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

d. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would violate the Privacy Rule if completed by Covered Entity.

7. Obligations of Business Associate upon Termination:

Upon termination of this BAA for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

a. Comply with the data transition requirements in the turnover plan as described in A.9 Turnover, including:

i. Transmit the PHI the Business Associate still maintains in any form;

ii. Whether the PHI / data will be destroyed without returning copies to Covered Entity or destroyed after returning copies to Covered Entity;

a) If destroyed, define the date Business Associate shall destroy any data related to this BAA; this date shall be known as the Retention Date;

b) If transferred to Covered Entity, define the following:

i) The date the transfer to Covered Entity or another Business Associate of Covered Entity shall occur; and,

ii) The format and method of transfer Business Associate will use to transfer all data pertaining to this BAA to Covered Entity – format and transfer method are subject to Covered Entity approval;

c) Execute the turnover plan to transfer the data to Covered Entity and/or destroy the data termination;

d) Obtain or ensure the destruction of PHI created, received, or maintained by subcontractors;

e) Destroy the PHI that Business Associate maintains in any form by an agreed upon date in the turnover plan; this date shall be known as the Retention Date.

f) All electronic storage media shall be disposed of in accordance with the media sanitation procedures outlined in the State of Oklahoma Information Security Policy, Procedures, Guidelines, Appendix E, Revision 3 that can be accessed at the following link: https://ok.gov/cio/documents/InfoSecPPG.pdf.

g) Business Associate shall send written certification of the destruction of all copies of data in Business Associate's and subcontractor's possession to Covered Entity within thirty (30 calendar) days of the destruction.

iii. Continue to use appropriate safeguards and comply with 45 C.F.R. Part 164, Subpart C with respect to PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains any PHI;

iv. Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions that applied prior to termination.

8. Survival:

The confidentiality, security, reporting, and indemnification obligations of Business Associate under this BAA, as well as any other obligations which by their nature would reasonably be expected to survive termination, shall survive the termination of this BAA.

9. Security and Privacy Controls:

a. Media Controls: In the event that data is exchanged via the Internet or File Transfer Protocol (FTP) reasonable encryption and the employment of authentication/identification techniques are required for use in safeguarding data. Furthermore, Covered Entity reserves the right to audit any organization's implementation of, and/or adherence to the requirements, as stated in this BAA upon seven (7) calendar days' notice during reasonable business hours. This includes the right to require that any organization utilizing the Internet or FTP for transmission of data submit documentation to demonstrate that it meets the requirements contained in this BAA.

b. Secure Transmission. Business Associate will only transmit Personally Identifiable Information, Protected Health Information, and other confidential or sensitive data by secure transmission that must implement encryption products that have been validated under the Cryptographic Module Validation Program (see http://csrc.nist.gov/groups/STM/cmvp/validation.html) to confirm compliance with current and successor FIPS cryptology requirements as they are made final, in accordance with applicable federal laws, directives, policies, regulations, and standards. For example, FIPS 140-2 Level 4 is the current requirement and Business Associate will comply with its successor publications when made final. Covered Entity will not provide additional hardware or software to Business Associate for this purpose, nor will Covered Entity accept any Business Associate provided hardware/software.

c. MARS-E Compliance. Business Associate agrees to comply with the latest version of the suite of documents entitled the Minimum Acceptable Risk Standards for Exchanges or "MARS-E." Alternatively, Business Associate agrees to implement and maintain standards that at all times meet or exceed the latest MARS-E requirements, for example NIST 800-53 rev 4 (moderate system) would meet the requirements of the current MARS-E. Business Associate further agrees to maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system with the highest security levels. If at any time, Supplier plans to implement and maintain security standards other than MARS-E or the most current applicable NIST standards referenced herein, Supplier must submit the specific details of the planned change to OHCA for approval not later than two (2) weeks before the date of planned implementation. If OHCA does not approve of the change, OHCA may elect to terminate the contract at any time upon written notice. In the event of such termination, OHCA shall not be subject to any damages, penalties, early termination fees, or other liabilities.

A.7 SOCIAL SECURITY ADMINISTRATION DATA, if applicable

1. Business Associate understands that the use, or disclosure of Social Security Administration (SSA) data in a manner or purpose not authorized by Covered Entity's agreement with the SSA (hereafter referred to as the "SSA Agreement") may be subject to both civil and criminal sanctions pursuant to applicable Federal statutes. Covered Entity will provide Business Associate with copies of the SSA Agreement, related Information Exchange Agreements (IEAs), and all related attachments. Business Associate will provide Covered Entity with a current list of the employees with access to SSA data and Covered Entity will provide the lists to SSA. It is also the responsibility of the Business Associate to immediately communicate any changes to this list to Covered Entity, no later than 24 hours following the change.
2. Business Associate agrees to abide by all relevant Federal laws, restrictions on access, use, disclosure, and the security requirements contained within the Covered Entity's agreement with SSA. For the purposes of this BAA, the Business Associate's staff with access to SSA-provided information, will use this access only as needed for the purposes stated in this BAA. Any other use is a violation of this BAA unless the additional use is specifically identified in a mutually accepted amendment executed in writing by the parties.
3. Business Associate shall report to Covered Entity and the SSA any security incident involving SSA data upon discovery within one (1) hour of knowledge of the incident. A Security Incident shall include, but is not limited to, unwanted disruption or denial of service, unauthorized use of a system for processing or storing SSA data, or changes to system hardware, firmware, or software without Business Associate's consent. Reports shall include successful Security Incidents.
4. The Business Associate agrees to follow the requirements of Covered Entity's data exchange agreement with SSA. Business Associate's employees will annually complete the Covered Entity security awareness training on the Covered Entity Learning Management System (LMS).
5. The Business Associate understands that Covered Entity is required by the SSA to conduct ongoing security compliance reviews that must meet SSA standards. The Covered Entity will conduct compliance reviews at least triennially commencing fiscal year 2019. Covered Entity will provide the documentation to the Business Associate following the review, and to SSA during Covered Entity's scheduled compliance and certification reviews or upon SSA's request.
6. The compliance reviews will be structured to ensure that the Business Associate meets SSA's requirements in the following areas:
    a. Safeguards for sensitive information;
    b. Computer system safeguards;
    c. Security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and redisclosure of SSA-provided information; and,

d. Continuous monitoring of Business Associate's network infrastructures and assets.

A.8 TURNOVER

Turnover is defined as those activities that Business Associate is required to perform upon termination of this BAA in situations in which Business Associate must transition contract operations to Business Associate or a third party. The requirements of this section are applicable upon termination or expiration of this BAA and any extensions.

1. General Turnover Requirements. In the event this BAA is terminated for any reason, Business Associate shall:
    a. Continue services until the effective termination date;
    b. Promptly supply all information necessary for Covered Entity to perform its operations; and
    c. Comply with direction provided by Covered Entity to assist in the orderly transition of services to Business Associate or a third party designated by Business Associate.
    d. Provide a draft Turnover Plan and work together with Covered Entity to develop the Turnover Plan.

2. Turnover Plan. Prior to the conclusion of this BAA, or in the event Business Associate's company ceases to do business or no longer exist, Business Associate shall provide, at no extra charge, assistance in turning over the data to Covered Entity or its agent or contractor.
    a. Timing: A draft Turnover plan is due to Business Associate within thirty (30) days from the date either party submits a notification of termination, unless other appropriate timeframes have been agreed upon by both parties. If this BAA is not terminated by written notification, Business Associate shall propose a Turnover Plan three (3) months prior to the end of the BAA period, including any extensions to such period.

    b. Content: The Turnover Plan shall address the turnover of records and information maintained by the Business Associate relative to services provided to Business Associate. The Turnover Plan must be a comprehensive document detailing the proposed schedule, activities, and resource requirements associated with the turnover tasks. The Turnover Plan must include, but is not limited to, at least the following:
        i. Proposed approach to turnover;
        ii. Identification of Covered Entity data and documentation in Business Associate's possession;
        iii. Description of the format and method of transfer Business Associate will use to secure encrypted transfer of all data pertaining to services performed for this BAA to Covered Entity or its agent/contractor;
        iv. Turnover tasks and schedule;
        v. A template turnover status report provided weekly (or as mutually agreed between the parties) until turnover is complete;
        vi. Acceptance criteria for successful turnover activities;
        vii. Estimated date certification of all data in Business Associate's possession will be turned over and all copies of data in Business Associate's possession will be destroyed; and
        viii. Method of destruction of all hosted information.
        ix. As part of the Turnover Plan, the Business Associate must provide Covered Entity with copies of all relevant data, documentation, or other pertinent information necessary, as determined by Covered Entity, for Covered Entity or a subsequent party to assume the services successfully. This includes correspondence, documentation of ongoing outstanding issues, and other operations support documentation. The Turnover Plan will describe the Business Associate's approach and schedule for transfer of all data and operational support information, as applicable. The information must be supplied in media and format specified by Covered Entity or as mutually agreed upon between the parties and according to the schedule approved by Covered Entity.

    c. Plan Approval: Covered Entity shall approve the Turnover Plan prior to Business Associate beginning turnover activities. Business Associate will work together with Covered Entity to develop a Turnover Plan acceptable to Covered Entity.

3. Transfer of Data. Business Associate shall transfer all data regarding the provision of services to Covered Entity or a third party, at the sole discretion of Covered Entity and as directed by Covered Entity or as mutually agreed between the parties. All transferred data must be compliant with HIPAA and HITECH.

   All relevant data must be received and verified by Covered Entity. If Covered Entity or its determines that not all of the data regarding the provision of services was successfully transferred, or the data is not HIPAA/HITECH compliant, Covered Entity reserves the right to require Business Associate to repeat the transfer attempt until transfer is successful, or to hire an independent contractor to assist Covered Entity in obtaining and transferring all the required data and to ensure that all the data are HIPAA/HITECH compliant. The reasonable cost of providing these services will be the responsibility of the Business Associate.

4. Documentation and Certification upon Turnover. At the turnover date, to be determined by Covered Entity, Business Associate shall provide to Covered Entity or its agent the following:
   a. All documentation and records as will be required by Covered Entity for continuity of services under this BAA; and,
   b. Certification that all data in Business Associate's possession has been turned over and all copies of data in Business Associate's (and its contractors') possession have been destroyed.

5. Post-Turnover Services. Thirty (30) days following turnover of operations, the Business Associate must provide Covered Entity with a Turnover Results report documenting the completion and results of each step of the Turnover Plan. Turnover will not be considered complete until this document is approved by Covered Entity.

   If the Covered Entity does not provide the required relevant data and reference tables, documentation, or other pertinent information necessary for Covered Entity or its contractor to assume the operational activities successfully, the Business Associate agrees to reimburse Covered Entity for all reasonable costs, for all state and federal representatives, or their agents, to carry out their inspection, audit, review, analysis, reproduction and transfer functions at the location(s) of such records. The Business Associate also must pay any and all additional costs incurred by Covered Entity that are the result of the Business Associate's failure to provide the requested records, data or documentation within the time frames agreed to in the Turnover Plan.

Remainder of page intentionally left blank.
Signature page follows.

Each party is signing this agreement on the date stated opposite that party's signature.

OKLAHOMA HEALTH CARE AUTHORITY d.b.a OKSHINE

By: _____ _____
Date

Print Name: _____

Title: _____

COVERED ENTITY NAME: _____

By: _____ _____
Date

Print Name: _____

Title: _____

EXHIBIT D – ANNUAL PARTICIPATION FEES

The annual participation fees for OKSHINE Participants is described below. These fees do not include implementation interface costs of organizational systems and vendors, if applicable.

OKSHINE pricing for hospital organizations is based on Adjusted Patient Days (APD). The base price is set on a sliding scale to accommodate small and large organizations. On average hospitals pay $0.79 per APD per month, but exact costs will be determined in coordination with the onboarding and outreach team.

OKSHINE pricing for provider clinics is based on the number of prescribing providers in each clinic. On average provider clinics pay $55 per prescribing provider per month, but exact costs will be determined in coordination with the onboarding and outreach team.

External data feeds or interfaces for HL7 ADT feeds or EHR based API / FHIR connections will be charged at a rate of $10K each. Specific needs and additional pricing will be determined in coordination with the onboarding and outreach team.

OKSHINE reserves the right to amend, terminate, or add additional Health Information Exchange (HIE) services at any time which may affect participant pricing upon thirty (30) days prior written notice to Participants consistent with the Policies and Procedures.

Invoicing for all participants will commence on July 1, 2022.

EXHIBIT E – OKSHINE AVAILABLE SERVICES

OKSHINE reserves the right to amend, terminate, or add additional Health Information Exchange (HIE) services at any time. The availability of OKSHINE Services to individual Participants is dependent on the State of Oklahoma certification, the technical capabilities of OKSHINE and Participant's organization.

Service	Description
Direct Secure Messaging (DSM) - Web-based and XDR	If requested, OKSHINE can provide Authorized Users with an ONC- compliant (Direct Trust-certified) Direct Secure Messaging service. Each Authorized User will be provided a unique address assigned in the OKSHINE Direct domain. OKSHINE maintains a Provider Directory Address Book of Direct Addresses in the OKSHINE Health Internet Services Provider (HISP) that is connected with a national director provided by DirectTrust. Please see fee schedule for web-based and XDR based DSM fees.
Clinical Portal/Query-based Exchange	OKSHINE provides Authorized Users access to OKSHINE Clinical Portal. This Portal can be used to view the longitudinal/community patient record, set alerts and notifications, and utilize other OKSHINE Services, including initiating a query of the eHealth Exchange to access additional clinical information that may be contained in other HIEs or Participants of the eHealth Exchange.
Alerts and Notifications	The OKSHINE Alerts and Notifications tools distribute relevant alerts and clinical information about pre-defined events such as hospital admissions, discharges, or finalized laboratory results available for review. As new event messages flow through OKSHINE, they may generate real-time notifications for delivery to subscribed users. Panel/roster-based Notifications are also available, ideal for Integrated Health Partnership care coordinators and for other use cases focused on attributed population-level use cases**. Utilizing OKSHINE for Notifications services enables Hospital Participants to meet the CMS ADT Notification Condition of Participation, which goes into effect in May 2021.**
eHealth Exchange	OKSHINE is a Participant of the eHealth Exchange and enables Participants to query the eHealth Exchange through the OKSHINE Clinical Portal.
Oklahoma Health Department (Registries and other OHD Reporting Services)	OKSHINE maintains a "public health gateway" with the Oklahoma Health Department (OHD) to enable integration with various MDH registries and reporting services. OKSHINE staff works closely with OHD to assist Participants with integration and onboarding and manages day-to-day operations for these transactions from Participant to/from OHD. **Some of these services include, but are not limited to**:

	Electronic Lab Orders/Results (Infectious Disease Lab): Multiplex Orders (COVID + Influenza) Bidirectional connection to **Immunization Registry** (MIIC)	**Electronic Lab Reporting** **electronic Case Reporting** (eCR) – AIMS Platform (CDC)

EXHIBIT F - OKSHINE POLICIES AND PROCEDURES

DEFINITIONS

For the purposes of the OKSHINE policies, the following terms shall have the meaning ascribed to them below. All defined terms are capitalized throughout the policies. Terms used, but not otherwise defined in OKSHINE policies, shall have the same meaning as those terms in 45C.F.R. §§ 160.103, 164.304 and 164.501.

APPLICABLE LAW: Applicable Laws include the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Acts and Regulations, Health Information Technology for Economic and Clinical Health Act (HITECH), Federal and State Laws and Regulations, and Administrative Rules applicable to Individually Identifiable Health Information.

ADMINISTRATIVE AUTHORIZED USER: Administrative Authorized User means individuals who have been authorized by the OKSHINE to perform services necessary for operating and maintaining the OKSHINE.

AUTHORIZED USER: Authorized Users are individuals who have been authorized by a Participant to participate in the OKSHINE HIE and may include, but are not limited to, health care practitioners, employees, contractors, agents, or business associates of a participant.

BREACH: Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Rules which compromises the security or privacy of the PHI.

BREAK THE GLASS: Break the Glass means the ability of an authorized user to access a patient's PHI after receiving or confirming the possession of written consent or in the case of a medical emergency.

BUSINESS ASSOCIATE: Business Associate has the meaning set forth in 45 C.F.R. 160.103 and generally means an individual or organization that creates, receives, maintains, or transmits PHI on behalf of a covered entity.

HIPAA: HIPAA means the Health Insurance Portability and Accountability Act of 1996. Specifically including the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic PHI (45 C.F.R. Parts 160 and 164) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009 and as any further amendments, modification, or renumbering which occurs or takes effect during the term of the policies.

HITECH means the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act, Pub. L. No. 111-5.

INDIVIDUAL: An Individual means a person who is the subject of PHI and has the same meaning as the term "Individual" in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION: Individually Identifiable Health Information means a subset of health information, including demographic information collected from an Individual, that is created or received by a health care provider or plan, employer, or healthcare clearinghouse, and relates to the past, present or future physical or mental health or condition or condition or payment for healthcare and that identifies or can be used to identify the Individual.

MEDICAL EMERGENCY: A Medical Emergency means a medical condition manifesting itself by acute symptoms of sufficient severity (including severe pain) such that the absence of immediate medical attention could reasonably be expected to result in:

1. placing the health of the individual (or, with respect to a pregnant woman, the health of the woman or her unborn child) in serious jeopardy, serious impairment to bodily functions, or;

2. Serious dysfunction of any bodily organ or part. This definition of a Medical Emergency Condition is found in the federal Emergency Medical Treatment and Active Labor Act (EMTALA) at 42 C.F.R. 489.24(b).

OKSHINE: The OKSHINE an organization that oversees, governs, and facilitates health information exchange among health care providers that are not related health care entities as defined in Oklahoma Statutes to improve coordination of patient care and the efficiency of health care delivery.

PARTICIPANT: A Participant means an organization, health care practitioner or institution, health plan, or health care clearinghouse who has executed a written Participation Agreement and Business Associate Agreement with OKSHINE.

PARTICIPATION AGREEMENT: Participation Agreement means the Agreement between OKSHINE and a Participant which authorizes the Participant to have access to OKSHINE.

PATIENT DATA: Patient Data means information that is requested, disclosed, stored, made available, or sent by a Participant through OKSHINE. This includes, but is not limited to, PHI, Individually Identifiable Health Information, deidentified data (health information that does not identify an individual as defined in C.F.R. § 164.514(a)) and Limited Data Sets (PHI that excludes certain identifier information as defined in 45 C.F.R. § 164.514(e)).

PROTECTED HEALTH INFORMATION AND ELECTRONIC PROTECTED HEALTH INFORMATION: Protected Health Information (PHI and ePHI) means Individually Identifiable Health Information (e.g., any oral or recorded information relating to the past, present, or future physical or mental health of an Individual; the provision of health care to the Individual; or the payment for health care) that is maintained by any medium and transmitted by electronic media or in any other form or medium.

SECURITY RULE: The Security Rule means the Security Standards for the Protection of Electronic PHI at 45 C.F.R. Part 160 and Part 164, Subparts A and C as may be amended from time to time.

UNSECURED PROTECTED HEALTH INFORMATION (PHI): Unsecured PHI means PHI in any form, including electronic, paper or verbal, that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in 45 C.F.R. § 164.402.

VENDOR: Vendor means Orion Health, or another entity selected by OKSHINE, to build and provide an electronic health information exchange system for Oklahoma.

RELIANCE: If an Individual's health information is available through the OKSHINE a Participant may assume the Individual has not opted-out of participation.

MINORS: In Oklahoma, a minor is a person under the age of 18 years. A parent or legal guardian of a minor may authorize release of the minor's health care information.

A minor, who may under Oklahoma law consent for certain treatment without parental consent, may restrict access to information relating to treatments that a minor may obtain without parental consent. In Oklahoma a minor may consent to treatment for pregnancy and associated conditions, venereal disease, and/or alcohol and drug abuse.

When a minor reaches the age of majority or is emancipated, access or exercise of control of the minor's health information by a parent or legal guardian will cease. When a minor reaches the age of 18 the minor has the right to participate or opt out of participation in the OKSHINE.

If a parent or legal guardian opted out of participation in the OKSHINE on behalf of the minor that election will remain in effect following the minor's reaching the age of majority until the Individual makes a change to a prior election.

POLICY 1: INCORPORATION OF POLICIES INTO AGREEMENTS

OKSHINE will maintain Policies (this document) which will be recognized as OKSHINE Privacy and Security Policies and Procedures, as referenced in OKSHINE Participation Terms and Conditions. These Policies will specify generally how OKSHINE will fulfill its obligations, and may be amended from time to time in accordance with the process specified in this Policy #1.

In addition, OKSHINE resources will develop, maintain, and amend, as needed, procedures which will correspond to these Policies for OKSHINE, Participants and Subscribers to depend on for details about the implementation of the policies. Said procedures will detail the process for OKSHINE resources, Participants and Subscribers (as applicable) to use to implement the Policies which apply to multiple OKSHINE Systems. Multiple procedures may be needed to implement certain policies depending on the application of each policy in different OKSHINE Systems.

Policies and procedures will be maintained in written (may be electronic) form. If an action, activity, or assessment is required to be documented, OKSHINE will maintain a written record of the action, activity, or assessment. OKSHINE will maintain the documentation of its active policies and procedures for 6 years from the date when they were in effect. OKSHINE will make the Policies publicly available and will make other documentation available to those persons responsible for implementing the policies and/or procedures to which the documentation pertains. OKSHINE will review all documentation periodically and update it as needed, in response to environmental or operational changes affecting the security of the electronic Protected Health Information (PHI).

DATA RESPONSIBILITY AND RECORD RETENTION

OKSHINE will retain the current version of PHI as provided to OKSHINE by Data Suppliers. "Current version" means the most complete record of patient data as provided by the Data Supplier, regardless of the age of that data. OKSHINE may also retain historical PHI.

OKSHINE is not responsible for retaining information used by clinicians for medical decisions. Authorized Users who use PHI from OKSHINE for patient care are responsible for making it part of their own medical records.

If a Participant Supplier leaves the OKSHINE, the PHI provided by the Participant Supplier will be returned or destroyed by OKSHINE if required by the Participant Supplier, and if possible, in accordance with OKSHINE Agreement. If a Subscriber Supplier leaves the OKSHINE, the PHI provided by the Subscriber Supplier will be handled in accordance with the terms of its Subscriber Agreement.

ASSIGNMENT OF OVERSIGHT RESPONSIBILITIES FOR THE OKSHINE

OKSHINE must appoint a Privacy Officer who will be responsible for compliance with and enforcement of the provisions of the HIPAA Privacy Rule. OKSHINE must appoint a Security Officer who will be responsible for compliance with and enforcement of the provisions of the HIPAA Security Rule.

COMPLIANCE WITH THE LAW AND OKSHINE POLICIES

These Policies must comply with the Terms and Conditions of OKSHINE Agreement signed by each Participant, to the extent the Terms and Conditions align with Applicable Law. Any conflicts between Policies and OKSHINE Agreement's Terms and Conditions, or differing interpretations, will be interpreted using the language of the most recently adopted document. The resolution of any issues that are not contemplated by OKSHINE policies or OKSHINE Agreement's Terms and Conditions, or conflicts over interpretation, will be resolved through OKSHINE governance structure. The final determination in such cases will be decided by OKSHINE Board of Directors.

OKSHINE and its Participants must comply with all applicable OKSHINE policies, and all applicable federal, state, and local laws and regulations including, but not limited to, the Information Blocking Rule, and those protecting the confidentiality and security of PHI and the establishing of certain individual privacy rights. These laws and regulations also include privacy principles of use limitation; security safeguards and controls; accountability and oversight; data integrity and quality; remedies; workforce training; sanctions for privacy/security violations, and the reporting of violations.

Participant Suppliers will be responsible for the content of the Data which they supply to the OKSHINE and have the responsibility to include the content that they are required to share in the Information Blocking Rule under the Content and Manner Exception –

Content condition at 45 CFR §171.301(a). OKSHINE may advise Participant Suppliers of potential compliance issues. OKSHINE will have the responsibility to comply with the content and manner requirements in the Information Blocking Rule only to the extent such information has been received by the OKSHINE. OKSHINE will require Subscriber Suppliers to be responsible for complying with the content and manner requirements in the Information Blocking Rule in connection with Data they supply to the OKSHINE.

OKSHINE and Participants will use reasonable efforts to stay abreast of any changes or updates to interpretations of such laws and regulations to ensure compliance. Internal policies and procedures will be promulgated as required to provide essential privacy protections for patients, and to avoid information blocking.
In the event of a conflict between OKSHINE policies and a Participant's own policies and procedures, the Participant must comply with the policy that is more protective of individual privacy and security, unless that policy would violate the Information Blocking Rule, in which case the Participant must comply with the policy that does not violate the Information Blocking Rule.

OKSHINE will require Subscribers to comply with their Subscriber Agreements, which must align with Subscriber obligations in these Policies, and applicable laws.

SANCTIONS AND ENFORCEMENT
OKSHINE and each Participant must maintain and enforce procedures to discipline and hold members of the Workforce accountable for failure to comply with OKSHINE policies. OKSHINE must impose sanctions on its Workforce members who are found to be non-compliant with these policies or any federal, state or local law. Such sanctions may include, but not be limited to, verbal or written warnings, required retraining, suspension without pay, and termination of contract or employment.

Any failure by a Participant's Workforce member to comply with a Participant's HIPAA Privacy and Security Policies will be handled according to the Participant's HIPAA Privacy and Security Policies.

Subscriber Agreements will require OKSHINE and Subscribers to comply with applicable law, with respect to maintaining and enforcing procedures to discipline and hold members of their own Workforce accountable for compliance with applicable laws.

OKSHINE Participants and Subscribers, to the extent provided by law, are responsible for the acts and omissions of their Workforce. OKSHINE will impose sanctions on a Participant or Subscriber whose Authorized Users fail to adhere to these Policies. Such sanctions may include, but not be limited to, verbal and written warnings, suspension of Data Recipient access or Data Supplier data feeds, mandated termination of individual Authorized User access, and termination of participation in the OKSHINE.

COMMUNICATION ABOUT POLICIES
OKSHINE will post information regarding privacy and security on its website to help inform the public regarding how key privacy and security issues are managed. Information for the public will be developed and monitored by the OKSHINE.

These Policies will also be posted on OKSHINE public website, for the benefit of Participants, potential Participants, and the general public, and must be kept current. They will be accessible at https://oklahoma.gov/ohca/OKSHINE /policies.

REVIEW AND AMENDMENT OF OKSHINE POLICIES
These Policies will be reviewed by OKSHINE Privacy Officer periodically, but at least annually, to determine compliance with applicable laws, regulations, and accreditation standards. Amendments to these policies may be proposed through the governance processes of the OKSHINE. Prior to proposing policy amendments, OKSHINE will consider to what extent Participants will in turn need to amend their Notices of Privacy Practices (documents required by HIPAA informing patients of how their PHI is being used) and will evaluate other impacts to OKSHINE Participants in conjunction with OKSHINE governance review process. These Policies may be amended by a vote of OKSHINE Board of Directors. OKSHINE must provide written notice to all Participants of any changes to the Policies at least thirty (30) days prior to the effective date of the change. However, if the change is required for OKSHINE and/or Participants to comply with applicable laws or regulations, OKSHINE may implement the change within a shorter period if OKSHINE determines it appropriate under the circumstances. OKSHINE must notify Participants immediately in the event of a change required to comply with applicable laws and regulations.

Participants may object to changes in accordance with Policy 2: Participant Objections for Amendments or Inter-HIO Expansion.

The preamble to the Policies is determined by the Board and are not subject to the above process.
REFERENCES:

- 45 CFR § 164.316
- 42 USC § 300jj-52, titled the “21st Century Cures Act”
- 45 CFR § 171.103(a)(2)
- 45 CFR § 171.201-203
- 45 CFR § 171.301(a)
- 24 Okla. Stat. § 161, et seq., titled the “Security Breach Notification Act.”
- OKSHINE Terms and Conditions 3.2, 10.3(b)(i) & (iii)

Effective Date: 10/8/2021
Latest Review Date: 10/8/2021

POLICY 2: SECURITY SAFEGUARDS

PURPOSE
The OKSHINE, it's Vendors, and each Participant shall be responsible for maintaining a secure environment that supports access to, use of, and the continued development of the OKSHINE.

SCOPE
This policy applies to all OKSHINE participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, and credentialed provider staff.

SAFEGUARDS
OKSHINE, its Vendors, and each Participant shall use appropriate safeguards to prevent the impermissible access, use or disclosure of Protected Health Information (PHI) other than as permitted by the OKSHINE policies, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of PHI through OKSHINE. Appropriate safeguards for OKSHINE, its Vendors, and Participants shall be those identified in the HIPAA Rules and other applicable federal and state standards and requirements, regardless of whether OKSHINE, its Vendors, and Participants are subject to HIPAA Rules. OKSHINE, its Vendors, and each Participant shall be responsible for requiring each of their Business Associates and Subcontractors to agree to comply with this Security Policy.

ADMINISTRATIVE AUTHORIZED USER
Definition: Administrative Authorized User means individuals who have been authorized by the OKSHINE to perform services necessary for operating and maintaining the access controls and user profiles of OKSHINE participants. OKSHINE Administrative Authorized Users and Participant Authorized Users will be granted access to the OKSHINE environment. All authorizing access will use the principle of "Least Privilege", that is, granting access to the minimal amount of resources required for the function that the user performs. A list of Authorized Users is maintained in the OKSHINE Participant Authorized User List. OKSHINE will verify each Participant's Authorized Users with Participant periodically. OKSHINE Administrative Authorized Users shall comply with OKSHINE Annual Security Awareness Training.

POLICY 3: SECURITY INCIDENT MANAGEMENT

PURPOSE
Provides guidelines to OKSHINE Participants for the identification and reporting of information security incidents.

SCOPE
This policy applies to all OKSHINE participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, and credentialed provider staff.

ROLES & RESPONSIBILITIES
It is the primary responsibility of OKSHINE participants and workforce to identify and respond to suspected or known security incidents in order to limit risk to exposure and mitigate harmful effects of such incidents.

OKSHINE will provide incident management training to all management staff on how to identify and report security incidents and how to continuously and proactively monitor for security incidents.

REFER TO BREACH MANAGEMENT AND NOTIFICATION POLICY FOR SPECIFIC REPORTING REQUIREMENTS DEFINITION OF SECURITY INCIDENT

For purposes of this policy, security "incident" means the act of violating an explicit or implied security policy, which includes unwanted disruption or denial of service, the unauthorized access to a system or its data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

While certain adverse events, (e.g. floods, fires, electrical outages, excessive heat, etc.) can cause system crashes, they are not considered incidents.

SEVERITY OF AN INCIDENT
When determining the scope of a security incident the following criteria will be considered:

- Scope of the impact
- Critical nature of the system or service that is affected
- Sensitivity and type of information accessed
- Likelihood that the negative impact will affect other systems or services or spread?

Response will be guided by the level of severity of the incident.

Level of Severity will be rated as – HIGH, MEDIUM, LOW AND NOT APPLICABLE

GUIDELINES FOR SECURITY INCIDENT RESPONSE:

HIGH SEVERITY INCIDENT: SIGNIFICANT ADVERSE IMPACT ON A LARGE NUMBER OF INDIVIDUALS OR SYSTEMS, PRESENTS A LARGE FINANCIAL RISK OR LEGAL LIABILITY OR THREATENS CONFIDENTIAL DATA OR A CRITICAL SYSTEM OR SERVICE.

RESPONSE: Requires immediate and focused attention by the OKSHINE Executive Director (ED), notification of legal and all department managers, incident response report and formal / extensive notification.

MEDIUM SEVERITY INCIDENT: DISRUPTS A BUILDING OR DEPARTMENT NETWORK, IMPACTS A MODERATE NUMBER OF INDIVIDUALS OR SYSTEMS OR IMPACTS A NON-CRITICAL SERVICE OR SYSTEM.

RESPONSE: Requires a quick response by personnel in the affected unit or department who have primary administrative responsibility within 4 hours of the incident, notification of the Executive Director, legal, affected department manager and an incident response report if requested by OKSHINE Executive Director.

LOW SEVERITY INCIDENT: IMPACTS VERY SMALL NUMBER OF INDIVIDUALS, SERVICES, NETWORKS OR BUSINESS SEGMENTS WITH NO RISK OF PROPAGATION AND LITTLE DISRUPTION.

RESPONSE: Response by the next business day, notify OKSHINE Executive Director and affected department manager, no incident report required unless the ED requests it for the purposes of tracking patterns or trends.

NOT APPLICABLE: USED FOR ANY SUSPECTED SECURITY INCIDENTS THAT ARE UNDER INVESTIGATION. REPORTING PROCEDURES OKSHINE participant or workforce member will immediately notify the OKSHINE Help Desk (405-522-7458) of any reportable security incident.

A ticket will be opened and notification of the appropriate resources will begin as stated above.
Each incident will be documented as per the OKSHINE BREACH MANAGEMENT AND NOTIFICATION POLICY and the record of that incident retained for at least one year or until the security incident is resolved.

OKSHINE will report security breaches affecting individuals within 60 days of the breach via email or postal service mail and HHS will be notified of any security breach that reaches the harm thresholds outlined in the HIPAA Security Rule.

OKSHINE REPORTING OF SECURITY INCIDENTS TO PARTICIPANTS
OKSHINE will report to a Participant any successful impermissible access, use, disclosure, modification, or destruction of Participant's electronic PHI or interference with system operations in an information system containing Participant's electronic PHI of which OKSHINE becomes aware, within five (5) business days of OKSHINE's learning of the event.

When feasible, OKSHINE will also report to a Participant the aggregate number of unsuccessful attempts of impermissible access, use, disclosure, modification, or destruction of electronic PHI or interferences with system operations in an information system containing electronic PHI of which OKSHINE becomes aware, provided that these reports will be provided only as frequently as the parties mutually agree.

RECOGNITION OF UNSUCCESSFUL ATTEMPTS – PROACTIVE MONITORING PROCEDURE
OKSHINE recognizes the number of unsuccessful attempts to the network, that is, remote access attempts without authorization.

- The number of unauthorized remote access attempts have a demonstrable effect on incident handling capability.
- Therefore, an "unsuccessful security event" is defined as one that does not result in unauthorized access, use, disclosure, modification, or destruction of electronic PHI or does not result in interference with an information system.
- No further notice of any such unsuccessful security event will be required.

References: 45 C.F.R. § 164.312 (c) (1-2), 45 C.F.R. § 164.312 (d), 45 C.F.R. § 164.312 (a) (1-2), 45 C.F.R. § 164.308 (3) (i), 45 C.F.R. § 164.308 (4) (i)

POLICY 4: INFORMATION SYSTEM AUDITS

PURPOSE
Audit procedures will be used to review information system activity to detect and minimize potential risks, vulnerabilities and security violations.

The OKSHINE shall conduct audits of health information accessed and used by Authorized Users to identify inappropriate access, verify compliance with access controls to assure confidentiality, verify appropriate use of Protected Health Information and assure compliance with HIPAA Rules, Oklahoma Statutes and OKSHINE policies.

SCOPE
Policy applies to all OKSHINE participants and workforce; participants, employees/authorized users, temporary staff, contracted staff, and credentialed provider staff.

Policy applies to all forms of PHI and includes system, application, and database and file activity whenever available or deemed necessary.

All activity will be logged from IT resources that store, access, maintain and transmit electronic PHI.

Whenever available audit logs will include creation, access, modification and deletion activity and the files will be retained for a period of no less than 12 months.

OKSHINE AUDITS
The OKSHINE shall periodically audit user authentication logs. Unusual findings must be investigated and resolved in a timely manner.

The OKSHINE must audit for “Break the Glass” activity, including auditing queries where written patient consent is affirmed, and review findings with the Participants.

The OKSHINE shall conduct periodic audits of Participant usage of OKSHINE services and upon request, shall provide the Participant with audit reports for their organization.

The OKSHINE may perform other Participant and Authorized User audits as it determines necessary.

Unauthorized access, use, or disclosure must be addressed by the OKSHINE ED or designee, by taking immediate and appropriate corrective measures including utilizing the OKSHINE Enforcement policy.

POLICY 5: ENFORCEMENT

The OKSHINE ED has the authority to suspend or terminate the access of any participant or authorized user in OKSHINE Health Information Organization under the following conditions:

EMERGENCY SUSPENSION
If the Vendor discovers a breach or suspicious transactions and considers it necessary to take immediate action, it may suspend access to the OKSHINE immediately. The Vendor shall notify the OKSHINE of the action, reason for its action, and collaborate with the OKSHINE ED to address the situation.

AUTHORIZED USER SUSPENSION OR TERMINATION
Upon the OKSHINE ED, or designee, completing a preliminary investigation and the OKSHINE ED determining that there is a substantial likelihood that an Authorized User's acts or omissions create an immediate threat or will cause irreparable harm to another party, including, but not limited to, a Participant, an Authorized User, the OKSHINE, Vendor, or an Individual whose health information is exchanged through OKSHINE, the OKSHINE ED, or designee, may suspend to the extent necessary to address the threat, the Authorized User's OKSHINE access.

A Participant may suspend, limit, or revoke the access authority of its Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's privacy or security policies, the OKSHINE policies, or the terms of the user agreement, if it is determined by the Participant to be necessary to protect the privacy of Individuals or the security of the system. The Participant must immediately notify the OKSHINE ED, or designee, of any action limiting access of an Authorized User.

The Participant responsible for the Authorized User shall take necessary steps to resolve the problems. Once resolved, the Participant shall notify the OKSHINE ED, or designee, and may request reinstatement of the Authorized User access.
The Participant must immediately notify the OKSHINE ED, or designee, of any change to an Authorized User's job responsibilities or a change of employment status or provider staff privileges, including every change in an Authorized User's access whether it opens, expands, restricts, or terminates the Authorized User's access to the OKSHINE.

PARTICIPANT SUSPENSION PROCESS
The OKSHINE ED, or designee, shall immediately but within twelve hours of suspending a Participant's access provide notice of the suspension and provide a written summary of the reasons for the suspension to the suspended Participant. The Participant shall use reasonable efforts to respond to the suspension notice with a detailed plan of correction or an objection to the suspension within three business days or, if such a submission is not reasonably feasible within three business days, then at the earliest practicable time.

Within five business days after submission of the Participants plan of correction, the OKSHINE ED, in collaboration with Vendor shall review and either accept or reject the plan of correction. If the plan of correction is accepted, the OKSHINE ED will, upon completion of the plan of correction, reinstate the Participant's access and provide notice to all Participants of the reinstatement. If the plan of correction is rejected, the Participant's suspension will continue, during which time the OKSHINE ED, Vendor, and the Participant shall work in good faith to develop a plan of correction that is acceptable to all. If agreement cannot be reached, either party may appeal the dispute to the OKSHINE Advisory Committee.

APPEAL PROCESS
A Participant may appeal, in writing, the OKSHINE ED's decision to suspend or terminate its participation in the OKSHINE to the Advisory Committee. The Committee shall review the written material from the Participant, Vendor, OKSHINE ED, or any affected party. The Committee may hold a meeting with the parties to gather additional information. The Committee shall issue a final determination, in writing, and the decision shall be provided to all Participants.

TERMINATION OF PARTICIPATION AGREEMENT
Upon any termination of the Participation Agreement the terminated party shall cease to be a Participant and neither it nor its Authorized Users shall have any rights to use the OKSHINE (unless the Authorized Users have an independent right to access the

OKSHINE through another Participant). The OKSHINE ED, or designee, shall immediately but within twelve hours of termination of a Participation Agreement provide notice of the termination to all Participants.

The OKSHINE shall retain an audit trail for a terminated Participant for at least six years.

Upon termination OKSHINE may no longer access or transmit any health information to and from the terminated Participant. Except as retained by other Participants, Vendor must delete or destroy any health information of the terminated Participant and certify the destruction to the OKSHINE ED and Participants.

GOVERNING LAW

In the event of a dispute between or among the parties to the OKSHINE, the laws of the State of Oklahoma will govern. Any action to enforce a Participation Agreement or participation in the OKSHINE must be adjudicated exclusively in the State of Oklahoma. Venue for civil actions arising out of this Agreement shall be in the District Court of Oklahoma County, Oklahoma.

Each Participant shall establish and enforce policies and procedures regarding Authorized User access to Patient Data (including Remote Access), the conditions that must be met and documentation that must be obtained prior to allowing an Authorized User access to Patient Data.

Policies shall include procedures for taking disciplinary actions for its Authorized Users or members of its workforce in the event of a breach or non-compliance with the OKSHINE policies.

POLICY 6: DATA ENCRYPTION

PURPOSE
To provide procedures for the protection of ePHI from destruction or alteration. This policy applies to all forms of ePHI maintained or transmitted by OKSHINE.

SCOPE
This policy applies to all OKSHINE participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, credentialed provider staff.

ENCRYPTION AT REST AND TRANSIT
The OKSHINE's vendor system shall employ Federal Information Processing Standards (FIPS) 140-2 compliant cryptography and cryptographic modules.

- All ePHI will be encrypted while stored and when in transit across open communications network.
- Mail messages containing ePHI transmitted outside the OKSHINE Intranet shall be encrypted and transmitted using an approved direct secure messaging protocol.
- All other ePHI transmissions shall be encrypted using approved mechanisms (Virtual Private Networks) whenever feasible or deemed necessary based on the findings of the most recent risk analysis or audit findings.

References: 45 C.F.R. § 164.312 (c) (1-2), 45 C.F.R. § 164.312 (d), 45 C.F.R. § 164.312 (a) (1-2), 45 C.F.R. § 164.308 (3) (i), 45 C.F.R. § 164.308 (4) (i)

POLICY 7: BREACH MANAGEMENT & NOTIFICATION POLICY

PURPOSE
To ensure that the impermissible or unauthorized use or disclosure of an Individual's Protected Health Information (PHI) will be reported and Participants shall comply with the notification requirements of 45 C.F.R. Part 164, Subpart D.

SCOPE
This policy applies to all OKSHINE participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, and credentialed provider staff.

DEFINITION OF BREACH
Breach means the acquisition, access, use, or disclosure of PHI , to include ePHI, in a manner not permitted under the HIPAA Rules which compromises the security or privacy of the PHI.

The impermissible or unauthorized acquisition, access, use, or disclosure ePHI is presumed to be a breach unless the covered entity or the business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved in the incident, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed or disclosed (re-disclosed); and
4. The extent to which the risk to the PHI has been mitigated.

EXCEPTIONS.
Breach does not include:

- Unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate.
- Inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.
- Good faith by the covered entity or business associate that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

REPORTING
Participants shall notify the OKSHINE of any breach of unsecured PHI in the most expedient time possible and without unreasonable delay but no later than five (5) calendar days following discovery.

OKSHINE will report to a Participant any use or disclosure of the Participant's ePHI that is not permitted. In addition, OKSHINE will report to the Participant, following discovery and without unreasonable delay, but in no event later than five (5) calendar days following discovery, any "breach" of "Unsecured PHI" as these terms are defined by the HIPAA Rules. OKSHINE shall cooperate with the Participant in investigating any suspected or known breach and assist in meeting the Participant's obligations under the Breach Notification Rule and any other state or federal privacy or security breach notification laws.

Any incident response report must include the following information, if known at the time of the report:

1. The identification of each Individual whose unsecured ePHI has been, or is reasonably believed by OKSHINE to have been, accessed, acquired, or disclosed during the breach, including their contact information if available to OKSHINE;
2. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
3. A description of the types of Unsecured ePHI involved in the breach (such as name, Social Security number, date of birth, home address, or account number);
4. The identity of any person who received the non-permitted PHI;
5. Any steps Individuals should take to protect themselves from potential harm resulting from the breach;

6. A brief description of what OKSHINE is doing or has done to investigate the breach, mitigate losses to Individuals and the Participant, and protect against any further breaches;
7. Contact procedures for Individuals to ask questions or learn additional information about the breach, which must include a toll-free telephone number and an e-mail, website, or postal address at OKSHINE; and;
8. Identification of the names and respective titles of those who conducted the investigation on the part of OKSHINE, be delivered on OKSHINE's official letterhead, signed by an officer or director of OKSHINE or other responsible person and contain appropriate contact information should the Participant need further clarification regarding the content of the report.

If deemed necessary by the Participant, OKSHINE may follow internal procedures to report directly to Individuals. Under this circumstance, OKSHINE will prepare a draft notice, and allow Participant(s) to provide input on and review the draft notice prior to it being sent; or conduct its own reporting, if so desired. If the required information is not known at the time of the initial report to a Participant or Participants, OKSHINE will follow up with an additional report or reports when the information becomes known until the time at which the incident response case is closed.

REPORTING IF MORE THAN ONE PARTICIPANT INVOLVED
If there is a breach of unsecured ePHI involving more than one Participant, OKSHINE will conduct the reporting on behalf of those Participants, so as to avoid duplicative reporting so long as Participant has reviewed and approved the draft notice. However, a Participant may conduct its own reporting if so desired. OKSHINE will make any required reports without unreasonable delay after approval of the content by Participant, if required, and in no event later than sixty (60) days after OKSHINE learns of the breach. However, OKSHINE may delay reporting if a law enforcement official determines that reporting will impede a criminal investigation or cause damage to national security, in which case reporting may be delayed in the same manner as provided under 45 C.F.R. § 164.528(a)(2).

OKSHINE will include the following information in the report to Individuals:
1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of Unsecured PHI involved in the breach (such as name, Social Security number, date of birth, home address, or account number);
3. A brief description of what OKSHINE is doing or has done to investigate the breach, mitigate losses to Individuals, and protect against any further breaches;
4. Steps Individuals should take to protect themselves from potential harm resulting from the breach; and
5. Contact procedures for Individuals to ask questions or learn additional information about the breach, which shall include a toll-free telephone number and an e-mail, website, or postal address at OKSHINE.

If the report mentions a Participant, the Participant has the right to approve the content of the report in advance, which approval the Participant may not unreasonably withhold.

REPORTING TO INDIVIDUALS
OKSHINE must provide the report to Individuals in writing, by first class mail, sent to the last known address of the Individual (or to the next of kin or personal representative if the Individual is deceased). If an Individual has specified a preference for electronic mail in communications with OKSHINE, then OKSHINE must use electronic mail. In any case in which there is insufficient or out-of-date information to provide the written notice required, OKSHINE must include a conspicuous posting on its website that includes a toll-free phone number so that affected Individuals may learn whether or not their Unsecured PHI may have been included in the breach.

REPORTING TO OKSHINE
Participant will immediately notify OKSHINE Help Desk at (844) 335-6253 (option 4) of any breach of Unsecured PHI.

REPORTING TO THE MEDIA

If OKSHINE believes that the breach of Unsecured PHI involved more than 500 Individuals residing within a State, OKSHINE also must provide notice to prominent media outlets serving that State. The media announcement must include a toll-free phone number so that Individuals may learn whether or not their Unsecured PHI may have been included in the breach.

REPORTING TO HHS
If OKSHINE believes that the breach of Unsecured PHI involved 500 or more Individuals, OKSHINE must also immediately notify the Secretary of the U.S. Department of Health and Human Services (HHS), and must indicate in its notice to HHS that the report is made on behalf of Participants in the OKSHINE to avoid duplicative reporting.

For breaches affecting fewer than 500 individuals, OKSHINE will maintain a log of all such breaches occurring during the year and annually submit such log to the Secretary.

RESPONSIBILITY OF VENDOR
If Vendor discovers a breach or suspicious transaction and considers it necessary to take immediate action, it may suspend the Authorized User's access to the OKSHINE immediately. Vendor shall notify the OKSHINE of the action, reason for its action, and collaborate with the OKSHINE ED, or designee, to address the incident.

OKSHINE RESPONSE TO A BREACH
The OKSHINE may conduct an investigation of the breach as outlined in SECURITY INCIDENT POLICY, to determine the extent of the breach, determine corrective actions, and may apply sanctions, as considered necessary. Participants shall cooperate in any investigation conducted by OKSHINE, state, or federal government authorities.

OKSHINE shall document its findings and any actions taken in response to an investigation. A copy shall be provided to the Participant.

SANCTIONS
OKSHINE ED may apply sanctions to Participants and their Authorized Users in the event of a breach. Sanctions may include restricting, suspending, or terminating a Participant or an Authorized User's access to the OKSHINE pursuant to the ENFORCEMENT POLICY, requiring Participants or Authorized Users to undergo additional training, requiring the Participant to develop a remediation plan, terminating a Participant's Agreement, or other remedies as the OKSHINE ED may reasonably deem necessary.

Each Participant, Vendor, or OKSHINE shall be respectively liable for any monetary penalties imposed as a result of a state or federal investigation and shall implement identified corrective actions at its expense.

PARTICIPANT POLICIES
Each Participant shall implement a process to mitigate, and shall mitigate to the extent practicable or required by law, the harmful effects that are known to the Participant of a known or suspected breach of access, use or disclosure of PHI.

Participants shall make this policy applicable to their business associates and their contractors and subcontractors.

RESPONSIBILITY TO eHealth Exchange
In addition to any other requirements, as OKSHINE joins the eHealth Exchange, the Participant agrees to comply with the provisions in Section 15.04 of the Restatement I of the Data Use and Reciprocal Support Agreement ("DURSA") that require the Participant:
To comply with all Applicable Law;

- To reasonably cooperate with OKSHINE regarding issues related to the DURSA.
- To Request, retrieve and send data only for a Permitted Purpose as defined in the DURSA (which is more restrictive than HIPAA);
- To use data received from OKSHINE or another eHealth Exchange Participant in accordance with the terms and conditions of the DURSA;
- To refrain from disclosing to any other person any passwords or other security measures issued to the Participant or to an Authorized User of the Participant by the OKSHINE; and
- To as soon as reasonably practicable, but no later than:

1. One (1) hour after discovering information that leads a OKSHINE Participant to reasonably believe that a Breach related to Transacting Message Content pursuant to the DURSA may have occurred, alert OKSHINE to the suspected breach; and
2. Twenty-four (24) hours after determining that a Breach related to Transacting Message Content pursuant to the DURSA has occurred, provide a Notification of any such Breach to OKSHINE;

In other words, if a breach (or suspected breach) occurs WHILE the Participant is sending, requesting, receiving, or accessing an electronic transmission of health information through the DURSA, the breach must be reported as required by this subsection. BUT IF the breach was from the Participant's EHR or electronic records system and did not occur WHILE (i.e., at the same time) the Participant or the Participant's Authorized user was using the DURSA (even though the information is ePHI received or accessed through the DURSA), the breach is considered to be not directly related to the DURSA and should not be reported under this subsection. (Although the Participant may be required to report the breach under other OKSHINE and HIPAA Notification rules).

As used in Subsection (6.) of the DURSA, "Transacting Message Content pursuant to the DURSA" means sending, requesting, receiving, asserting, responding to, submitting, routing, subscribing to, or publishing information contained within an electronic transmission of health information transacted by an OKSHINE Participant using the DURSA Specifications, including any information contained in an electronic transmission, or accompanying any such transmission such as Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonyms level (partially de-identified) data, metadata, Digital Credentials, and schema.

The Notification of a DURSA breach should include sufficient information for OKSHINE to understand the nature of the Breach. For instance, the Notification could include, to the extent available at the time of the 24-hour Notification, the following information:

- One or two sentence description of the breach
- Description of the roles of the people involved in the breach (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
- The type of Message Content breached
- Participants likely impacted by the breach
- Number of individuals or records impacted or estimated to be impacted by the breach
- Actions taken by the Participant to mitigate the breach
- Current Status of the breach (whether under investigation or resolved)
- Corrective action taken and steps planned to be taken to prevent a similar breach.

The Participant shall supplement the information contained in the Notification as it becomes available and cooperate with other Participants and OKSHINE in investigating and taking corrective action in response to the breach.

The requirements do not apply to any acquisition, access, disclosure or use of information contained in or available through the DURSA if the acquisition, access, disclosure or use:

- Is not directly related to Transacting Message Content through the DURSA; or
- Is an unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of the OKSHINE or Participant if—
- The acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the OKSHINE or Participant and
- The Message Content is not further acquired, accessed, disclosed or used by that employee or individual.

The requirements are addition to and do not supersede a Participant's obligations, if any, under relevant security incident, breach notification, or confidentiality provisions of the Participation Agreement, the Participant's Business Associate Agreement with OKSHINE, the HIPAA Rules, or other applicable law.

POLICY 8: USE AND DISCLOSURE OF HEALTH INFORMATION

PURPOSE
To comply with Oklahoma State Law and HIPAA requirements for the use and disclosure of protected health information (PHI) on behalf of OKSHINE participants.

SCOPE
This policy applies to all OKSHINE participants and workforce; participants, employees/ authorized users, temporary staff, contracted staff, and credentialed provider staff.

COMPLIANCE WITH LAW
All disclosures and uses of health information through the OKSHINE HIE must be consistent with all applicable federal and state laws and OKSHINE policies. Disclosures and uses may not be used for any unlawful or discriminatory purpose. If applicable law requires that certain documentation exist (such as an authorization or consent) or that other conditions be met prior to using or disclosing health information for a particular purpose. In all cases, the requesting OKSHINE participant shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of the documentation and conditions at the request of the disclosing Participant.

PARTICIPANT PERMITTED PURPOSES
A participant may request and may disclose individual health information through the OKSHINE with a signed consent from the individual and only for purposes of treatment, payment, health care operations, or to comply with public health reporting requirements and as required by law.

Each OKSHINE Participant shall provide or request Protected Health Information (PHI) through the HIO only to the extent necessary for the permitted purpose.

Any other use of Individually Identifiable Health Information data is prohibited.

Business Associates should refer to the BA Use & Disclosure of Health Information Policy.

OKSHINE PERMITTED PURPOSES
OKSHINE may use and disclose Protected Health Information (PHI) for the following purposes:

- _for the proper management and administration of the Business Associate, in accordance with 45 C.F.R. § 164.504(e)(4);
- _subject to the Participation Agreement, OKSHINE policies and procedures, and 45 C.F.R. §§ 164.504(e)(2)(i) and 164.504(e)(2)(i)(B), provide data aggregation services related to the health care operations of the covered entities with which OKSHINE has a Participation Agreement;
- _manage authorized requests for, and disclosures of, PHI among Participants in the network;
- _create and maintain a master patient index;
- _provide a record locater or patient matching service;
- _standardize data formats;
- _implement business rules to assist in the automation of data exchange;
- _facilitate correction of errors in health information records; and
- _subject to the OKSHINE Participation Agreement and policies and procedures, aggregate data on behalf of multiple covered entities.

PROHIBITIONS
Except as permitted by Oklahoma State Law and the HIPAA Rules, Patient Data may not be used by OKSHINE or their participants for marketing, marketing related purposes, or sales without the authorization of the Individual or the Individual's designated representative.

INFORMATION SUBJECT TO SPECIAL PROTECTION

Certain health information may be subject to special protection under federal, state, or local laws and regulations (e.g., substance abuse). Each Participant shall identify any information that is subject to special protection under applicable law prior to disclosing any information through OKSHINE. Each Participant is responsible for complying with all applicable laws and regulations.

MINIMUM NECESSARY 45 CFR 164.502(B), 164.514(D)

The HIPAA Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. Protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information.

The minimum necessary standard does not apply to the following:

- _Disclosures to or requests by a health care provider for treatment purposes.
- _Disclosures to the individual who is the subject of the information.
- _Uses or disclosures made pursuant to an individual's authorization.
- _Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- _Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- _Uses or disclosures that are required by other law.

Each Participant may share health information through OKSHINE and allow access to the information by only those workforce members, business associates, and other authorized agents who need the information in connection with their job function or duties.

TREATMENT AND INSURANCE DENIAL PROHIBITION

A health care practitioner may not deny a patient health care treatment and a health insurer may not deny a patient a health insurance benefit based solely on the provider's or patient's decision not to participate in OKSHINE.

PARTICIPANT POLICIES

Each OKSHINE Participant shall have in place and shall comply with its own internal policies and procedures regarding the use and disclosure of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making any such disclosure.

POLICY 9: PRIVACY AND DATA PRACTICES

OKSHINE PROTECTS HEALTH INFORMATION
OKSHINE complies with patient privacy rights in accordance with state law and the Privacy and Security Regulations enacted under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

If substance abuse and addiction treatment information is protected by federal law, it is not available to any other health care provider unless specific patient consent is obtained in these situations, or in the case of a medical emergency.

REVISION OF PARTICIPANT NOTICE OF PRIVACY PRACTICES
Each Participant shall revise its notice of privacy practices (the "Notice") to describe the uses and disclosures of protected health information contemplated through the Participant's participation in OKSHINE, if such a use and disclosure is not already addressed in the Notice.

The Notice must meet the content requirements set forth under the HIPAA Privacy Rule and comply with applicable laws and regulations. Participants shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through OKSHINE.

OKSHINE provides the following sample language for Participants who elect to amend their Notice: "We may make your protected health information available electronically through an electronic health information exchange to other health care providers that request your information for their treatment and payment purposes. Participation in an electronic health information exchange also lets us see their information about you for our treatment and payment and healthcare operation purposes. You are permitted to request and review documentation regarding who has accessed your information through the electronic health information exchange. Your provider will have information on how to make this request, or you may find the information at https://oklahoma.gov/ohca/hie.html

Participants may elect more stringent language but may not commit OKSHINE to any additional obligations or liabilities through the Notice.

OKSHINE INFORMATION
At the point of care, an Individual or Individual's representative must be provided with written information in plain language about information exchange and OKSHINE. The material shall describe the benefits of participation, risks of participation, how and where to obtain additional information, contact information, and a description as to how the Individual's health information will be used.

In Oklahoma individuals must be informed that they have the right to opt-out of participation in the Record Locator Service so that their health care records are not found or located as a mechanism to preserve an individual's right to privacy. Individuals have a right to change a prior election and must be provided information on how to exercise those options, at no cost to the Individual. If an Individual later changes a prior election, the Participant receiving the new election shall maintain that documentation and shall notify OKSHINE of the change.

OPT-OUT
If an Individual opts out of participation in the OKSHINE, that Individual's information will not be able to be searched for through OKSHINE in the future. Minimal identifying information about the Individual will also be maintained in master patient index.

A Participant may not withhold coverage or care from an Individual on the basis of that Individual's choice to opt out of participation in OKSHINE.

POLICY 10: AMENDMENT OF DATA

PURPOSE
To ensure that individuals maintain the right to request an amendment of their protected health information.

SCOPE
This policy applies to all OKSHINE participants and workforce; participants, employees /authorized users, temporary staff, contracted staff, and credentialed provider staff.

ACCEPTING REQUESTS FOR AMENDMENTS
If an Individual requests an amendment to the individual's Protected Health Information, OKSHINE shall forward the request to the Participant that created the documentation and inform the individual requesting the amendment that the request was transferred to that Participant.

Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information.

INFORMING OTHER PARTICIPANTS
If the Participant that created the information accepts the requested amendment, in whole or in part, the covered entity as required by 45 C.F.R. 164.526(c) must make reasonable efforts to inform and provide the amendment within a reasonable time to: (i) persons identified by the individual as having received Protected Health Information about the individual and needing the amendment; and (ii) persons, including business associates, that the Participant knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on that information to the detriment of the individual.

APPLICATION TO BUSINESS ASSOCIATES AND CONTRACTORS
Participants shall make this policy applicable to their Business Associates ("BA") and to the contractors and subcontractors of their BAs as required by the HIPAA Rules.

POLICY 11: COMPLAINT PROCESS POLICY

PURPOSE
The OKSHINE provides a complaint process for any Individual or Participant to register a complaint.

DEFINITIONS
Authorized Users are individuals who have been authorized by a Participant to participate in the HIO and may include, but are not limited to, health care practitioners, employees, contractors, agents, or business associates of a Participant.

Individual means a person who is the subject of Protected Health Information (PHI) and has the same meaning as the term "Individual" in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

Participant means an organization, health care practitioner or institution, health plan, or health care clearinghouse who has executed a written Participation Agreement and Business Associate Agreement with the OKSHINE.

WHO MAY FILE A COMPLAINT
An Individual or a person on behalf of an Individual may file a complaint concerning:

- the impermissible use, disclosure or disposal of Protected Health Information
- denials of access to Individual Protected Health Information
- retaliation against an individual for filing a complaint
- A Participant or its Authorized Users, or member of the OKSHINE workforce may file a complaint concerning the following issues:
- violation of policies and procedures
- the impermissible use, disclosure or disposal of Protected Health Information
- retaliation against an individual for filing a complaint

COMPLAINTS RELATING TO A PARTICIPANT OR ITS AUTHORIZED USERS
Each Participant shall implement a process for workforce members, agents, contractors and Individuals to report any non-compliance with policies and a process for Individuals whose health information is shared through OKSHINE to file a complaint with the Participant about impermissible disclosures and uses of information about them.

The Participant shall investigate the complaint and shall provide a written response to the complainant. The response must include information about how the complainant may forward the complaint to OKSHINE if the complaint concerns OKSHINE.

COMPLAINTS RELATING TO THE OKSHINE
The complaint must be in writing and contain the complainant's name and contact information. No personal health information should be included. Verbal complaints will not be accepted by OKSHINE. Anonymous complaints will not be accepted by OKSHINE. A Complaint Form is available at https://oklahoma.gov/ohca/okshine/resources.html or can be requested by calling OKSHINE at 405-522-7458. The complaint form may be submitted by mail or electronically (see instructions on form).

If the complaint relates to a suspected violation or breach of PHI, the complaint must be filed within 180 days from the date of becoming aware of a suspected violation.

Upon receipt of a written complaint, it will be immediately forwarded to:

OKSHINE PRIVACY OFFICER
c/o Oklahoma Health Care Authority
4345 N Lincoln Blvd
Oklahoma City, OK 73105

OKSHINE shall acknowledge receipt of the complaint within 2 business days.

OKSHINE shall issue a written response to the Individual or Participant within 30 days of receipt of the complaint, unless under extenuating circumstances, OKSHINE may extend this deadline and provide the Individual or Participant written notification of the delay.

The response must include information about how the complainant may forward the complaint to the Oklahoma Healthcare Authority, which oversees the health information exchange program in Oklahoma.

If the complaint relates to OKSHINE, the complaint shall be reviewed by the OKSHINE Privacy Officer and a designated sub-committee of the OKSHINE Advisory Committee. All complaints will be duly investigated, findings documented and final disposition communicated back to complainant.

If the complainant is not satisfied by the OKSHINE investigation, findings, and any proposed resolution of the complaint, the complainant may send the complaint to the OKSHINE Advisory Committee via the ED and may forward complaint to the Oklahoma Healthcare Authority, which oversees the health information exchange program in Oklahoma.

The final disposition of a complaint shall be documented by OKSHINE.

GENERAL
OKSHINE will maintain the confidentiality of the Individual who files a complaint.

OKSHINE shall not retaliate, discriminate against, intimidate, coerce, or threaten any person who files a complaint.

Documentation concerning a complaint including response and resolution shall be maintained by OKSHINE for at least six (6) years.

OKSHINE shall periodically analyze filed complaints to determine if persistent or recurrent problems exist and make recommendations to correct identified problems.

FILING A COMPLAINT WITH U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Individuals are encouraged to file a complaint with a Participant or the OKSHINE to resolve an issue. However, an Individual or a person on behalf of an Individual may also file a complaint with the Secretary of the U.S. Department of Health and Human Services, Office of Civil Rights, within 180 days from the date of becoming aware of a suspected violation of the Individual's Protected Health Information or privacy rights.

POLICY 12: ACCESS CONTROL POLICY

PURPOSE
To protect an Individual's health information from unauthorized use, the OKSHINE shall verify the identity of Participants and their Authorized Users before access to OKSHINE is granted. Health information available through OKSHINE shall be accessed only by Authorized Users who have been granted access rights.

SCOPE
This policy applies to all OKSHINE participants and workforce; participants, employees / users, temporary staff, contracted staff, and credentialed provider staff.

AUTHENTICATION
Authentication is the process of verifying that an Authorized User who is seeking to access information through the OKSHINE is the individual who the Authorized User claims to be.

PARTICIPANT AUTHENTICATION
The OKSHINE ED, or designee, and each Participant shall execute a written and signed OKSHINE Participation Agreement prior to the Network access.

The OKSHINE shall review, evaluate and act upon requests submitted by organizations that want to become a OKSHINE Participant.

- Each OKSHINE Participant must demonstrate that it is a legitimate business by completing an application and provide the requested information. The OKSHINE participant must assure that its agents and workforce access ePHI for only valid business reasons and that it participates in the types of health care transactions required of a Covered Entity or its Business Associate.
- The OKSHINE ED, or designee, in collaboration with the OKSHINE participant shall determine whether the entities meet technical and operational requirements and pass the readiness assessment.
- OKSHINE Participant identity shall be authenticated, and unique usernames and passwords shall be assigned by OKSHINE to Authorized Users identified by Participant.
- Each OKSHINE Participant shall designate its responsible contact person (e.g., department manager) who shall be responsible on behalf of the Participant for compliance with OKSHINE policies and to receive notice on behalf of the Participant. Access rights shall be properly authorized and documented by the participant contact and access rights will be periodically audited to ensure compliance.
- OKSHINE Participants shall, within five (5) working days, notify OKSHINE if there is a material change in status such as a change in ownership or change in job assignment. If the Participant ceases to engage in health care transactions, it shall notify OKSHINE at least 30 days before the change.
- Participants shall notify OKSHINE within twenty-four hours, of termination of an Authorized User's employment or affiliation with the Participant.
- Only information technology staff at OKSHINE or system administrators are permitted to create or change access control settings.

AUTHORIZED USERS
OKSHINE Participants shall designate the Authorized Users within their organizations who will be authorized to access information through the OKSHINE. Participants shall develop and implement policies to assure proper identification of each Authorized User.

- Authorized Users shall be required to execute a user agreement prior to network access.
- Authorized Users must maintain a current relationship with a Participant to access the OKSHINE.

Access to health information shall be based on the Authorized User's job function and relationship to the patient. Categories of Authorized Users shall be established, at a minimum, as the following:

1. Practitioner with access to clinical information and "Break the Glass" authority.
2. Practitioner with access to clinical information but no "Break the Glass" authority.
3. Non-practitioner with access to clinical information.

4. Non-practitioner with access to non-clinical information.

OKSHINE Administrative Authorized Users shall be based on the job functions. Categories of OKSHINE Administrative Authorized Users shall be established, at a minimum, as the following:

1. Administrative Authorized User with access to non-clinical information.
2. Administrative Authorized User with access to clinical information to resolve technical issues or input advance directives received from third parties.
3. Administrative Authorized user with access to clinical information for audit purposes.

PASSWORDS

Each Authorized User shall be assigned a unique username and an initial password that is required to be changed at the next use by OKSHINE.

Passwords shall meet the strong password guidelines set forth in this OKSHINE Access Control Policy.

1. Authorized Users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing the last 5 passwords.
2. Password must be a minimum of eight characters and contain a combination of upper-case letters, lower case letters, and special characters.
3. Password should not be a word found in the dictionary (English or foreign).
4. The password should not be a name, initials, birthdays or phone number associated with authorized user.

Authorized Users are prohibited from sharing their usernames and passwords with others and from using the usernames and passwords of others.

OKSHINE shall encrypt user authentication data stored in the Network.

FAILED ACCESS ATTEMPTS

The OKSHINE shall enforce a limit of consecutive failed access attempts by an Authorized User. Upon the 5th failed attempt, OKSHINE shall disable the Authorized User's access to the OKSHINE. The Authorized User may reestablish access using appropriate identification and authentication procedures established by the Participant.

PERIODS OF INACTIVITY

The OKSHINE will have an automatic log-off and will terminate an electronic session after 30 minutes of inactivity. A Participant may establish a shorter automatic log-off and termination period for an electronic session on its network or for any device or class of devices used by its Authorized Users to access the Participant's network.

TRAINING

Participants shall provide training for all of its Authorized Users consistent with the Participant's and OKSHINE policies including privacy and security requirements.

PARTICIPANT POLICIES/REMOTE ACCESS

Each OKSHINE Participant shall establish and enforce policies and procedures regarding Authorized User access to Patient Data (including Remote Access), the conditions that must be met and documentation that must be obtained prior to allowing an Authorized User access to Patient Data.

Policies shall include procedures for taking disciplinary actions for its Authorized Users or members of its workforce in the event of a breach or non-compliance with the policies.

The OKSHINE Participant may suspend, limit, or revoke the access authority of an Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's policies or the OKSHINE policies. The OKSHINE Participant shall inform the OKSHINE office immediately, and in any case within twenty-four hours, of any revocation or suspension.

OKSHINE AUTHENTICATION

OKSHINE shall authenticate users accessing the OKSHINE with each attempt the user accesses the Network.

References: 45 C.F.R. §164.308 (3) (i), 45 C.F.R. §164.308 (3) (i), 45 C.F.R. §164.312(d), 45 C.F.R. §164.312(a) (1-2).

POLICY 13: PATIENT RIGHTS AND PREFERENCES

PURPOSE:
OKSHINE values the Individual's right to privacy. OKSHINE also values having the right information about the right patient available to the right provider at the right time in the right setting. This policy discusses how OKSHINE aims to balance these values.
As used in this policy, Individual means the person who is the subject of the PHI, as defined in 45 CFR § 160.103. An Individual's personal representative is one who has authority to act on behalf of the Individual who is the subject of the PHI, according to the criteria defined in 45 CFR § 164.502(g).

COMPLIANCE WITH LEGAL REQUIREMENTS
PHI will be used, accessed, created, and disclosed only as permitted under the HIPAA Privacy Rule. With regard to HIPAA, OKSHINE stores and manages Individuals' PHI as a Business Associate of its Data Suppliers under the terms of OKSHINE Agreements (for Participants), and under the terms of Subscriber Agreements (for Subscribers), which will conform with the guidelines for Subscribers as outlined in these Policies. Storage of data on behalf of Participant Suppliers is not a Disclosure (45 CFR § 164.501). For Sensitive Information—as defined in the Glossary—Data Suppliers are responsible to obtain appropriate authorization from the Individual or the Individual's personal representative prior to submitting such PHI to the OKSHINE and must provide documentation of such authorization to other OKSHINE Participants upon request.

OKSHINE 'S RESPECT FOR PATIENT PRIVACY PREFERENCES
OKSHINE provides a method for any Individual, or an Individual's personal representative (as defined in 45 CFR § 164.502(g)) to opt out of the sharing of their PHI through the OKSHINE, as well as a method to revoke the opt-out request.
Minors may make their own opt-out requests in instances in which they may legally consent for their own health services, as outlined in 63 Okla. Stat. §2602 A (1)-(7), 42 CFR Part 2, or other applicable law, as verified by the Participant.
Providers and payers must not condition treatment or coverage on an Individual's willingness to permit access to their PHI through the OKSHINE.

INFORMING PATIENTS ABOUT THE OKSHINE
OKSHINE must provide information about an Individual's option to opt out or to revoke the opt-out request, along with the necessary forms in OKSHINE office, and on OKSHINE website in a prominent position. The website, the opt-out form and the opt-out revocation form must describe the effect of opting out in plain language, with complete instructions for submitting the form. Participants will make available to Individuals information about how their data may be accessed via health information exchange, and the option and process to opt out utilizing OKSHINE -provided or OKSHINE -approved educational materials in ways that can reasonably be expected to be seen by Individuals in the due course of their interaction with Participants. Participants are responsible for accurately representing the opt-out opportunity to Individuals and may provide additional patient education opportunities with their notice of privacy practices, or other methods in cooperation with the OKSHINE. Subscribers will be required to provide transparency for patients so they can be informed that their data is being shared through OKSHINE, and that they have the right to opt out in information they make available to Individuals about privacy.

Some Data Suppliers, such as behavioral health facilities, may provide additional patient preference policies based on their technical and procedural capabilities. However, compliance with any additional patient preferences beyond those supported by OKSHINE is the responsibility of the individual Data Supplier, and not of the OKSHINE.

PROCESS OF OPTING OUT OR REVOKING THE OPT-OUT REQUEST
An Individual or an Individual's personal representative may opt out, or may revoke an opt-out request, at any Participant location or through means accommodated by a Participant or Subscriber, by completing and submitting the appropriate standard form provided by the OKSHINE, or a compatible substitute for the form that has been approved by OKSHINE and that correctly communicates the effect of the opt-out choice. The Participant or Subscriber receiving the form or its substitute must verify that the Individual's information is complete, including identity, must sign the form or otherwise authorize its substitute in an approved way by the OKSHINE, and immediately forward the form or its substitute to the OKSHINE. Alternatively, an Individual or an Individual's personal representative may opt out, or may revoke an opt-out request, by completing and submitting the appropriate standard form, which is provided at OKSHINE website, or by any Participant or Subscriber, then signing and having the form notarized by a

Notary Public and mailing or delivering to OKSHINE as instructed on the form. An Individual's personal representative who submits a notarized form must also supply evidence of his or her authority to act on behalf of the Individual.

Opt-out requests that are properly completed and submitted according to the instructions on OKSHINE standard form, or according to an approved substitute procedure, must be processed immediately during business hours, upon receipt by the OKSHINE. Then, OKSHINE will mail a letter to the Individual's provided address, confirming action on the Individual's request.

If required information is absent or illegible, the form or its substitute has been altered, or the request is unable to be honored for any reason, OKSHINE will communicate, as necessary and appropriately, with the requesting Individual or the Individual's personal representative as well as the submitting Participant or Subscriber, if applicable, and as appropriate, in order to resolve the issue that is preventing the request from being honored.

OKSHINE must retain a copy of each opt-out or opt-out-revocation form received, or records of the substitutes received, with a record of the corresponding actions taken.

EFFECT OF OPTING OUT

To opt out means that an Individual's PHI will be inaccessible to Data Recipients and to parties of authorized HIO-to-HIO data sharing relationships (as described in Policy 9) through OKSHINE Systems, except for the Individual's demographics, and for exceptions outlined below. An Individuals' demographics must remain accessible to identify records associated with the Individual to which the opt-out request applies, and to otherwise manage essential activities in OKSHINE System.

When an Individual's opt-out request is revoked, the Individual's PHI, both past and present, regardless of the Individual's opt-out status at the time the PHI was produced, becomes available to Data Recipients through OKSHINE Systems.

An Individual's opt-out request within OKSHINE will be global, meaning that the request to opt out is applied to all Participants, Subscribers, HIO-to-HIO interfaces, other connections, and applications which OKSHINE has the ability to control.

CLARIFICATIONS REGARDING THE SCOPE OF THE EFFECT OF OPTING OUT

An Individual's request to opt out of OKSHINE does not prevent health care professionals from communicating with one another about the care of the Individual.

Application functionality that facilitates Health Care Operations (meaning the activities specified in 45 CFR §164.501 to the extent that the activities are related to covered functions of the Participant), including the use of De-identified Data for quality improvement activities, is not restricted based on an Individual's opt-out request.

EXCEPTIONS TO UNAVAILABILITY OF PHI FOR INDIVIDUALS WHO OPT OUT

EXCEPTION: ACCESS TO PHI IN AN EMERGENCY SITUATION

Some of OKSHINE applications may provide the ability for specified Authorized Users to declare an Emergency Situation (defined below) and override an Individual's opt-out request on this basis. In applications where this capability exists, the Authorized User with the appropriate access role may access an opted-out Individual's PHI by attesting that it is an Emergency Situation, and that the treating practitioner has determined that PHI that may be held by OKSHINE system may be material to treatment. In such cases, the Authorized User must acknowledge that the access event will be closely reviewed and that additional information about the incident may be required at a later date.

In such cases, an Authorized User's right to access PHI in an Emergency Situation terminates with the completion of the emergency treatment.

OKSHINE must maintain a record of all such emergency access, and involved Participants, Subscribers, and OKSHINE may review each instance of emergency access.

An “Emergency Situation” is defined as a situation in which there appears to be an “Emergency Medical Condition” as defined in 42 USC section 1395dd (e)(1). For reference, that term is currently (as of this policy review date) defined as follows: a medical condition manifesting itself by acute symptoms of sufficient severity (including severe pain) such that the absence of immediate medical attention could reasonably be expected to result in placing the individual’s health or the health of an unborn child in serious jeopardy, serious impairment to bodily functions, or serious dysfunction of bodily organs.

EXCEPTION: PATIENT-AUTHORIZED IMMEDIATE OPT-IN ACCESS
Some of OKSHINE applications may provide the ability for specified Authorized Users to attest that a patient has signed an authorization for revocation of their opt-out request and has requested it take effect immediately. In applications where this capability exists, the Authorized User with the appropriate access role may access an opted-out Individual’s PHI by attesting that the Individual or the Individual’s personal representative has completed and submitted the proper opt-out revocation form (or its substitute), and briefly describing the situation justifying the need for immediate access.

In such cases, the Participant must process the opt-out revocation form (or its substitute) according to applicable procedures. OKSHINE must maintain a record of the authorized immediate opt-in access and will review if the accompanying form (or its substitute) is not received in accordance with the applicable procedures.

EXCEPTION: PUBLIC HEALTH REPORTING
If a Data Supplier is permitted or required to disclose PHI to a government agency for the purpose of public health reporting without an Individual’s consent under applicable state and federal laws and regulations, OKSHINE may make that disclosure on behalf of the Data Supplier even if an Individual has requested to opt out.

REFERENCES:
- 45 CFR § Part 164
- 45 CFR § 164.312(a)(2)(ii): Emergency Access Procedure
- 42 CFR Part 2
- 42 CFR § 489.24
- 42 CFR § 2.11
- 63 Okla. Stat. §2602 A (1)-(7)
- American Medical Association Policy H-140.989
- OKSHINE Terms and Conditions Section 10.3(d)(iii)

POLICY 14: MALICIOUS SOFTWARE & VIRUS PROTECTION

PURPOSE
To detect, guard against and have formal procedures in place for the reporting of malicious software and virus protection. SCOPE This policy applies to all OKSHINE participants and workforce; participants, employees / authorized users, temporary staff, contracted staff, and credentialed provider staff.

SECURITY CONTROLS TO MITIGATE RISK OF MALWARE AND VIRUS DISRUPTION
OKSHINE, their Vendor, and each OKSHINE Participant shall ensure that it employs security controls that meet applicable industry or Federal standards.

The intent of security controls is so that information being transmitted and any method of transmitting such information will not introduce any malware or other program designed to disrupt the proper operation of a system, the network or any part thereof, or any hardware or software used by the OKSHINE, Vendor, and each Participant in connection therewith.

In the absence of applicable industry standards, OKSHINE, Vendor, and each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.

In addition, Malware (Virus) protection shall be installed and activated on all applicable OKSHINE resources. This includes all computer equipment kept up to date with operating systems security software patches and fixes.

OKSHINE Vendor will regularly check that software is in place and up-to-date for all OKSHINE systems to identify spyware, viruses, worms, Trojans and other forms of various malicious software.

POLICY 15: PARTICIPANT OBJECTIONS FOR AMENDMENTS OR EXPANDED DATA SHARING

Purpose: The governance structure of OKSHINE is designed to invite Participants to be engaged in the decision-making processes of the OKSHINE. However, in the case that a Participant objects to amend the Policies, or in the case that a Participant objects to the terms for sharing Data or for compliance with applicable laws that are contained in a new agreement made by OKSHINE (which OKSHINE may make in accordance with Policy 9: Use and Disclosure of PHI), a Participant may object within 30 days.

Policy: When the Board of Directors votes to amend the Policies, or when OKSHINE authorizes the exchange of PHI under a new contractual arrangement, such as a Subscriber Agreement or an Inter-HIO Agreement, notification of the change must be made to the Authorized Administrators of each Participant.

If a Participant determines that the change affects one of its material rights or obligations under its Agreement, and the Participant objects to the change, the Participant may, within thirty (30) days following OKSHINE notice of the change to the Participant, (a) make request to OKSHINE for reconsideration, noting the reasons for the Participant's objection; (b) request to have Participant's PHI excluded if their objection relates to an exception under the Information Blocking Rule; or (c) if the objection is based on an amendment to Policies (and not based on a new agreement made by OKSHINE for sharing Data), Participant may terminate its OKSHINE Agreement by giving OKSHINE written notice thereof, which may be effective immediately unless a future date is agreed upon with the OKSHINE.

When an objection is raised to a particular Policy amendment, the change will be rolled back, or will not—if possible—be implemented with respect to the objecting Participant, until resolution of the reconsideration request or the stated effective date of termination, unless such change is required for OKSHINE and/or Participants to comply with applicable laws or regulations.
When an objection is raised to a new contractual arrangement for OKSHINE to exchange PHI, the data sharing arrangement will not—if possible—be implemented with respect to the objecting Participant, until the Participant's objection has been addressed under this Policy.

Request for Reconsideration or exclusion based on a Policy amendment:
In the event a Participant requests reconsideration or exclusion based on a policy amendment, the Board of Directors must review the request and make a determination thereon within sixty (60) days of its receipt of the request. The determination must be finalized and must be conveyed in writing to the Participant at least five (5) business days prior to becoming final.

Request for Reconsideration or exclusion based on a new data sharing arrangement:
In the event a Participant requests reconsideration or exclusion based on a new data sharing arrangement, OKSHINE must review the request and finalize a determination thereon before proceeding with the data sharing arrangement in a way that would affect Participant, unless required to proceed with the data sharing arrangement under applicable law. If OKSHINE is required to proceed with the data sharing arrangement under applicable law, OKSHINE will take any possible steps to limit the impact to Participant and will advise Participant of the actions being taken and why.

To finalize the determination, OKSHINE will propose its determination in writing to the Participant, the proposed determination will become final in five (5) business days, unless OKSHINE agrees in writing to extend the consideration time frame or OKSHINE and Participant agree in writing to finalize the determination. After a determination has been finalized, OKSHINE may proceed with the new data sharing arrangement, consistent with the finalized determination.

Termination Based on Objection:
In the event a Participant chooses not to request reconsideration or exclusion or is still unsatisfied based on the response or determination to Participant's request, Participant may, within 30 days, terminate its OKSHINE Agreement by giving OKSHINE written notice of termination pursuant to this policy and/or the terms of its OKSHINE Agreement. Such termination will be effective upon receipt of the notice, unless a future date is agreed upon between OKSHINE and the Participant.

References:
Policy 1: OKSHINE Policies, Compliance, Responsibilities and Updates
Policy 9: Use and Disclosure of Protected Health Information (PHI)

Effective Date: 10/8/2021
Latest Review Date: 10/8/2021
Revision History:

POLICY 16: ANALYTICS AND RESEARCH

PURPOSE:
In accordance with OKSHINE stated purpose to reduce the cost and improve the quality and efficiency of health care, OKSHINE aggregates data, including PHI, from Data Suppliers. This policy governs the uses and disclosures of PHI used for any purpose consistent with HIPAA and other Applicable Law not otherwise permitted by OKSHINE policies, including research, as those are referenced in Policy 8: Use and Disclosure of Protected Health Information (PHI).

POLICY:
OKSHINE must maintain a Board-authorized process for review and approval of proposed data uses and/or disclosures for any purpose consistent with HIPAA and other Applicable Law, including the Information Blocking Rule, not otherwise permitted by OKSHINE policies, including research, as these purposes are defined in Policy 9: Use and Disclosure of Protected Health Information (PHI). This process will apply to the development and use of reporting and analytics services involving Community Data, meaning data from multiple Participant Suppliers, and will satisfy the requirements of the approvals required to enable each of the uses that will be defined and adopted in OKSHINE Terms and Conditions. This process will also include provisions to properly review and route requests based on approvals which are required for each request. Data Suppliers may require that their data undergo approval of an Institutional Review Board ("IRB") or similar type of designee prior to their data being included in the result of one or more approved data requests.

Participants in OKSHINE may submit requests for datasets. Participant requests for datasets derived from information that is available to them in the Provider Portal which are for Permitted Purposes, as described in Policy 9, must be submitted on a standard request form and may be filled by OKSHINE without further approvals from committees or the Board. For all other requests, prior to making a request, a Participant seeking to receive or sponsor the dataset ("Requestor") must:

- Complete a standard request form provided by the OKSHINE.
- Obtain, where possible, necessary IRB review and approval.
- Counsel with OKSHINE 's Workforce to gain feedback and assistance in preparing the request for committee consideration.

Requestors are advised that requests submitted to OKSHINE may require several iterations through committees to obtain full approval. After a request has been submitted to the OKSHINE, requests must be reviewed by, and must be approved by each of the following, in order:

- Operations Management Committee
- OKSHINE Board of Directors

Depending on the details of the request, additional approvals may be required from one or more of the following:

- One or more Institutional Review Boards
- Affected Data Suppliers
- Affected Individuals
- Other stakeholders

All reports or services must comply with all applicable Business Associate Agreements and permitted uses. Unless otherwise specified, approved report templates may be reused without requiring new approvals if being used by the same entities for the same purposes with the same parameters.

OKSHINE may withdraw authorization for an approved report at any time without prior notice to the report recipients but shall only do so in compliance with the Information Blocking Rule.

REFERENCES:

- OKSHINE Terms and Conditions Sections 1.2, 9
- Policy 9: Use and Disclosure of Protected Health Information (PHI)

Effective Date: 10/08/2021
Latest Review Date: 10/08/2021

Revision History:

POLICY 17: INTEROPERABILITY WITH NON-PARTICIPANTS

FULFILLING REQUESTS TO ACCESS, EXCHANGE, OR USE EHI
PURPOSE:
This policy describes how OKSHINE will ensure compliance with the Information Blocking Rule when requests are received that constitute requests by requestors of OKSHINE as an actor and establishes how OKSHINE will accommodate basic data exchange under a limited license, referred to in these Policies by the term Subscriber.

POLICY:
Under the Information Blocking Rule, OKSHINE is a "health information exchange," as that term is defined in 45 CFR §171.102, and is therefore an actor who is required to refrain from practices that constitute Information Blocking as defined under the Information Blocking Rule. A requestor may make a request for EHI from OKSHINE for particular content, which is EHI, to be delivered in a particular manner, as outlined in 45 CFR §171.301 (Content and Manner Exception).
When such requests occur, OKSHINE will respond in the following ways:
If the request is already permitted under an existing Participation Agreement or Subscriber Agreement, OKSHINE will fulfill the request in accordance with the terms of the applicable Agreement.

If the request is not already permitted under an existing Participation Agreement or Subscriber Agreement, then:
OKSHINE will determine if the request is allowable under the Information Blocking Rule, in accordance with the regulations in the Information Blocking Rule. OKSHINE shall establish, in consultation with Participant Suppliers, a procedure which shall be used for assessing requests. This procedure will incorporate methods for ascertaining whether the EHI being requested:

1) Meets the "Preventing Harm Exception" (45 CFR §171.201)
2) Meets the "Privacy Exception" (45 CFR §171.202)
3) Meets the "Security Exception" (45 CFR §171.203)
4) Meets the "Content and Manner Exception" (45 CFR §171.301)
5) Is addressable within the criteria allowed by the "Fees Exception" and the "Licensing Exception" (45 CFR §§171.302-303)
6) Meets the "Infeasibility Exception" (45 CFR §171.204)
7) Meets the "Health IT Performance Exception (45 CFR §171.205)

If the request for EHI meets one or more of these exceptions, OKSHINE will follow the process prescribed in the Information Blocking Rule to attempt and resolve the issues to enable Interoperability to occur.

If OKSHINE determines a request is not allowable, OKSHINE will communicate this finding and the reason to the requestor, in accordance with the Information Blocking Rule.

If OKSHINE determines a request is allowable then:
OKSHINE will begin negotiation with the requestor within 10 business days from the receipt of the request and will negotiate a license with the requestor within 30 business days from the receipt of the request, as required in 45 CFR §171.303 (Licensing Exception).

If the requestor is a Participant requesting expanded access than is currently permitted under an existing Agreement, OKSHINE will work with the Participant to incorporate the desired license under the terms of the existing Agreement, and thus addressing the request.

If the requestor is not a Participant, the license OKSHINE negotiates will take the form of a Subscriber Agreement, which must be consistent with the terms of these Policies that pertain to Subscribers and must have a means to remain consistent with these Policies when these Policies are amended. OKSHINE will attempt to act in the best interests of OKSHINE and its Participants to negotiate licenses where Subscribers also act as Subscriber Suppliers, so EHI can be exchanged bidirectionally between Subscribers and Participants.

If the requestor is requesting EHI as an Individual or for an Individual, or on the basis of an Individual's authorization. OKSHINE will respond in accordance with Policy 22: Requests for Access to Records by an Individual.

OKSHINE will summarize and report on pending, new and existing Subscriber agreements to the Operations Management Committee.

REFERENCES:

- 45 CFR § 171

Effective Date: 10/08/2021
Latest Review Date: 10/08/2021
Revision History:

POLICY 18: REQUESTS FOR ACCESS TO RECORDS BY AN INDIVIDUAL

PURPOSE:
This policy describes how OKSHINE will ensure compliance with the Information Blocking Rule when requests are received that constitute requests for EHI by an Individual, for an Individual, or on the basis of an Individual's authorization.

POLICY:
If OKSHINE receives requests for EHI for the purposes of sharing with an Individual, or for the purpose of disclosing to another party on the basis of an Individuals' authorization, OKSHINE will engage in the negotiation required by the Information Blocking Rule and will also collaborate with Data Suppliers for the purpose of ensuring the requested EHI is not subject to one of the exceptions under the Information Blocking Rule. If OKSHINE establishes, with help of Data Suppliers, that no exceptions apply, OKSHINE will fulfill the request through the process outlined in Policy 21, Fulfilling Requests to Access, Exchange, or Use EHI.

REFERENCES:
- 45 CFR § 171

Effective Date: 10/08/2021
Latest Review Date: 10/08/2021
Revision History: