ARKANSAS OFFICE OF HEALTH INFORMATION TECHNOLOGY (OHIT) PRIVACY POLICIES

OHIT wishes to express its gratitude to Connecting for Health and the Markel Foundation for their work in developing the Common Foundation: Resources for Implementing Private and Secure Health Information Exchange and NEHII, Inc. This work incorporates some of the concepts set forth in those resources.

TABLE OF CONTENTS

Page

POLICY 100: COMPLIANCE WITH LAW AND POLICY 7
POLICY 200: NOTICE OF PRIVACY PRACTICES..... 9
POLICY 300: INDIVIDUAL CONTROL OF INFORMATION AVAILABLE THROUGH SHARE 10
POLICY 400: ACCESS TO AND USE AND DISCLOSURE OF INFORMATION..... 13
POLICY 500: INFORMATION SUBJECT TO SPECIAL PROTECTION 16
POLICY 600: MINIMUM NECESSARY 18
POLICY 700: WORKFORCE, AGENTS, AND CONTRACTORS..... 20
POLICY 800: AMENDMENT OF DATA..... 22
POLICY 900: REQUESTS FOR RESTRICTIONS 23
POLICY 1000: MITIGATION 24
POLICY 1100: INVESTIGATIONS; INCIDENT RESPONSE SYSTEM..... 25
POLICY 1200: AUTHORIZED USER CONTROLS 27

OHIT Privacy Policies

INTRODUCTION

The following policies apply to the access, use and disclosure of protected health information by Participating Entities through the Office of Health Information Technology (OHIT) State Health Alliance for Records Exchange ("SHARE") and other data exchange services being made available to Participating Entities. SHARE and these other services are collectively referred to as the "System." These policies are designed for use as SHARE and its Participating Entities exchange health information. It is anticipated these policies will be reviewed and revised as needed based on the experience of OHIT and Participating Entities.

STATUS OF OHIT AND PARTICIPATING ENTITIES

The following terms used throughout the policies are defined as follows:

Participating Entities means those entities which provide data to SHARE and those entities which obtain and use data from SHARE as health care providers, health plans, or health care clearinghouses (collectively "Covered Entities" as defined by HIPAA[1]). All Participating Entities are Covered Entities under HIPAA or have signed Participation Agreements with OHIT. Participating Entities should not be confused with Individuals whose protected health information is exchanged using SHARE.

Business Associate means one who acts for, or on behalf of a Participating Entity to perform a function or activity involving the use or disclosure of protected health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or any other function or activity, See 45 CFR §160.103.

OHIT is a business associate ("BA") of the Participating Entities who are Covered Entities under HIPAA. OHIT accepts and agrees to follow terms applicable to the privacy of protected health information by virtue of its business associate agreements with Participating Entities and these privacy policies.

Individual(s) means those persons whose protected health information is transmitted using SHARE.

[1] 45 C.F.R. §160.103.

PRIVACY PRINCIPLES

These OHIT Privacy Policies ("Privacy Policies") are rooted in nine privacy principles discussed in the **Connecting for Health** "The Architecture for Privacy in a Networked Health Information Environment" and a tenth adapted from NeHII, Inc. by OHIT that, taken together with privacy policies and procedures already deployed by Participating Entities as Covered entities under HIPAA form a comprehensive array of administrative safeguards addressing privacy of protected health information. OHIT has modeled its Privacy Policies on the **Connecting For Health** "Model Privacy Policies and Procedures for Health Information Exchange," with a number of differences based on state law, physical and technical safeguards available through SHARE, and SHARE's unique operating environment.

These core privacy principles and the policies that flow from them promote balance between consumer control of and access to health information and the operational need of covered entities to ensure that information uses and disclosures are not overly restricted, such that consumers would be denied many of the benefits and improvements that information technology can bring to the health care system. The policies are intended to reflect a carefully balanced view of all of the principles and avoid emphasizing some over others in any way that would weaken the overall approach. The guiding OHIT privacy principles are as follows:

Openness and Transparency. Clarity about procedures, policies, developments, and technology concerning the handling of protected health information is vital to protecting privacy. Individuals should be able to understand what information exists about them, how the protected health information is used, and how they can control use of that information. Openness and transparency helps promote privacy practices and gives individuals confidence with regard to privacy of protected health information, which in turn can help increase consumer participation in health information networks.

Purpose Specification and Minimization. Access to and use of patient health information must be limited to the type and amount necessary to accomplish specified permitted purposes. Minimizing the use of protected health information will help decrease the amount of privacy violations, which may occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

Disclosure Limitation. Protected health information should be made available through SHARE to OHIT and Participating Entities only by lawful means, and, if applicable, with the knowledge and permission of the individual. Electronic collection of protected information may be confusing to most individuals. It is important that individuals are aware of how information concerning them is being collected in an electronic networked environment. Individuals should be educated about the potential health and treatment benefits as well as risks to their protected health information that are associated with participation in SHARE. Individuals deciding not to participate should have the opportunity to know the System-wide effect of such decision and the potential disadvantages.

Access and Use Limitation. Protected health information should be obtained by one Participating Entity from another only pursuant to mutual agreement that the information is being accessed for qualifying treatment or payment purposes of the requesting Participating Entity or for other purposes permitted by law. Participating Entities may use and disclose protected health information obtained through SHARE only for purposes and uses consistent with their permitted access and consistent with their obligations as covered entities under HIPAA. Certain exceptions, such as for law enforcement or public health reporting, may warrant disclosure of information for other purposes. However, when information obtained by a Participating Entity through SHARE is used for purposes other than those for which the information was originally obtained, the Participating Entity so using or disclosing the information should first apply the rules applicable to it as a Covered Entity under HIPAA and as a contracting Participating Entity.

Individual Participation and Control. Consistent with the scope of individual rights in HIPAA, individuals should have the right to request and receive in a timely and intelligible manner information regarding various parties that may have that individual's specific health information; to know any reason for a denial of such request; to request to amend any protected health information that the individual believes is inaccurate; and to request not to have his or her information made available through SHARE. Individuals have a vital stake in their protected health information, such rights enable individuals to make informed decisions about participation and provide another means to monitor for inappropriate access, use and disclosure of protected health information. Individual participation promotes information quality, privacy, and confidence in privacy practices.

Data Integrity and Quality. Health information should be detailed, complete, appropriate, and current to guarantee its value to the various parties. The effective delivery of quality health care depends on complete health information. In addition, individuals can be negatively affected by inaccurate health information in other contexts, such as insurance and employment. Therefore, SHARE must maintain the integrity of protected health information and individuals must be allowed to view information about them and request to amend such health information so that it is accurate and complete.

Security Safeguards and Controls. In an era of increased computer and Internet-related crime, security safeguards are vital to privacy protection. Networked environments could be susceptible to cyber-crime without adequate controls. Such controls are put in place to prevent information loss, corruption, unauthorized use, modification, and disclosure. Methods of precaution that can be implemented include information scrubbing, identity management tools, hashing, auditing, authenticating, and other means to ensure information privacy. Privacy and security safeguards should be coordinated for the protection of patient health information.

Accountability and Oversight. Privacy protections have less value to an individual if privacy violators are not held accountable for failing to follow procedures relating to such privacy protections. Potential Participating Entities, such as those who will provide data to SHARE, are unlikely to fully trust SHARE and fully participate, if they

believe other Participating Entities are not applying the same rules and being held to the same standard of accountability. User and workforce training, privacy audits, and other oversight tools can help to identify and address privacy violations and security breaches by conditioning participation and access authority on compliance with these and the individual Participating Entity's privacy policies, by excluding from participation those who violate privacy requirements, and by identifying and correcting weaknesses in privacy and security safeguards.

Remedies. To ensure privacy protection there must be legal and financial remedies that hold violators accountable for failing to comply with OHIT policies. Such remedies will give individuals confidence in the organization's commitment to keeping protected health information private, and mitigate any harm that privacy violations may cause individuals. As a condition of continued participation, all Participating Entities in SHARE must have a common duty to participate in investigation, mitigation and remediation steps for the integrity of SHARE.

Reliance on Covered Entity Policies and Enforcement. While OHIT should have a number of core policies and procedures for the benefit and confidence of all Participating Entities, OHIT should not try to replace policies, procedures and methods already adopted by Participating Entities as covered entities under HIPAA. OHIT should identify, disseminate and enforce only those policies and procedures necessary for coordination of privacy response, but should recognize that existing Participating Entity policies govern in all other areas.

OHIT policies incorporate the principles outlined in the preceding ten principles as well as basic requirements set forth in HIPAA. The OHIT policies seek to achieve a balance between maintaining the confidentiality of health information and maximizing the benefits of such information.

EFFECT OF LEGISLATION AND RULE CHANGES

OHIT and Participating Entities need to remain flexible in approach in order to adapt to the uncertainty of state and federal legislation and regulations that will affect design, safeguards, rights and responsibilities over time. This shall include monitoring and implementing design components and safeguards mandated in the Health Information Technology for Economic and Clinical Health Act or "HITECH" as enacted in P.L 111-5 and regulations to be issued thereunder.

SAFEGUARDS IN AN ELECTRONIC NETWORKED ENVIRONMENT

HIPAA permits covered entities that hold protected health information to disclose such information to other covered entities both for their own treatment and payment purposes and for the treatment and payment purposes *of such third parties, without written authorization.*[2] HIPAA limits authority to disclose without authorization in other situations and attaches conditions. HIPAA thus places a duty on Participating Entities

[2] 45 C.F.R. §164.506(c) (2) (3) and (4).

holding protected health information to determine that each proposed disclosure is permitted.

In a non-electronic health care environment, Participating Entities subject to this duty would have the opportunity to examine third party requests for information beforehand and make an individual determination whether a disclosure is a permitted disclosure for the treatment or payment purposes of the requesting Participating Entity. In an electronic health care environment, such as SHARE, the disclosing Participating Entity will not receive or "process" a request for access. Other Participating Entities using SHARE can simply locate the Participating Entity's record and access it as needed. The human element of analyzing individual requests is absent.

Accordingly, to permit Participating Entities that furnish information to meet their obligation to disclose protected health information only for a qualifying purpose, and to meet certain other conditions during the initial phase of SHARE, including the responsibility to do the following:

- Access information from another Participating Entity's records only for a qualifying treatment or payment use by the requesting Participating Entity. A qualifying treatment or payment use is one that would permit the Participating Entity from whose records the information is accessed to disclose such information to the requesting Participating Entity under §§164.506(c)(2) and (3) of the Privacy Rule.

- Access information by applying the minimum necessary standards as defined by HIPAA.

To support this approach, OHIT and the Participating Entities will ensure that the all Participating Entities must be covered entities under HIPAA or have signed a Participation Agreement with OHIT and therefore are individually subject to regulation and penalties.

- During its initial phase, all Participating Entities commit to accessing PHI only for their treatment and payment purposes. While §164.506(c)(4) permits limited disclosure for the health care operations of another Participating Entity, SHARE is only to be used by Participating Entities to access protected health information for treatment and payment purposes or for public health reporting purposes. As SHARE matures, OHIT is authorized to develop Privacy and Security Procedures to address uses and disclosures which are not for treatment, payment, operations or public health reporting including requests for research purposes in accordance with state and federal regulations.

"Treatment" and "payment," as used in these policies and explanations, have the meaning given in Section §164.501 off the Privacy Rule.

OHIT Privacy
Policy 100: Compliance with Law and Policy

Scope and Applicability: This Policy applies to OHIT and all Participating Entities.

Policy:

1. **Laws.** Each Participating Entity must, at all times, comply with all federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of protected health information and establishing certain individual privacy rights. Each Participating Entity must use reasonable efforts to stay up-to-date of any changes or updates to and interpretations of such laws and regulations to ensure compliance.[3]

2. **OHIT Policies.** Each Participating Entity shall, at all times, comply with these OHIT Policies ("OHIT Policies"). These OHIT Policies may be changed and updated from time to time upon reasonable written notice to Participating Entities. Amendments shall be effective when adopted by the OHIT with review by the SHARE Health Information Exchange Council and promulgated as required by the Arkansas Administrative Procedures Act. OHIT shall notify Participating Entities of all policy changes. Each Participating Entity is responsible for ensuring it has, and is in compliance with, the most recent version of these OHIT Policies.

3. **Participating Entity Policies.** Each Participating Entity is responsible for establishing internal policies that are necessary to comply with applicable laws and these OHIT Policies.

4. **Participating Entity Criteria**. Each Participating Entity shall itself be a HIPAA Covered Entity or have executed a Participation Agreement with SHARE. Therefore, each Participating Entity will have either a legal duty as a regulated Covered Entity under HIPAA or have contractually assumed obligations under its Participation Agreement. Each Participating Entity must commit to be a data provider to the extent possible in order to become a data user.

5. **User Criteria.** Authorized users are individuals who have been granted access authority. Each authorized user derives his or her permission to access and use SHARE from a Participating Entity. Therefore each authorized user must maintain a current relationship to a Participating Entity in order to use SHARE. Authorized users must therefore be: (i) Participating Entities (for example, an individual physician) or workforce of a Participating Entity, (ii) an individual Business Associate (BA) or workforce of such BA, or (iii) an individual contractor or subcontractor of a BA or workforce of such contractor or subcontractor. Additionally, a Participating Entity that is a covered health plan may also be an authorized user in its role as a third party administrator and BA for self-funded

[3] The Participants acknowledge the need to revise Policies and certain other technical and administrative features to conform to HITECH and regulations to be promulgated thereunder.

group health plans that are covered entities under HIPAA but are not themselves Participating Entities.

6. **Application to BAs and Contractors.** Participating Entities shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

OHIT Privacy
Policy 200: Notice of Privacy Practices

Scope and Applicability: This Policy applies to all Participating Entities.

Policy:

Each Participating Entity who is a Covered Entity under HIPAA shall develop and maintain a notice of privacy practices (the "Notice"). The Notice must describe the uses and disclosures of protected health information contemplated through the Participating Entity's participation in SHARE.

1. **Content.** The Notice must meet the content requirements set forth under the HIPAA Privacy Rule[4] and comply with applicable laws and regulations. Participating Entities shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through SHARE. OHIT provides the following sample language for Participating Entities 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 and health plans 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 purposes. "

2. **Dissemination and Individual Awareness.** Each Participating Entity shall have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgment of receipt by the individual, [5] which policies and procedures shall comply with applicable laws and regulations.

3. **Participating Entity Choice.** Participating Entities may choose a more proactive Notice distribution or patient awareness process than provided herein and may include more detail in their Notice, so long as any expanded detail does not misstate the safeguards supporting SHARE.

[4] 45 C.F.R. § 164.520 (b).
[5] See 45 C.F.R. § 164.520(c) (2) (ii).

OHIT Privacy
Policy 300: Individual Control of Information Available Through SHARE

Scope and Applicability: This Policy applies to OHIT, SHARE, and all Participating Entities.

Policy:

1. **Choice Whether to Have Information Included in SHARE**. All individuals will have the opportunity to allow their protected health information to be exchanged using SHARE as well as the opportunity to opt out of allowing their protected health information to be exchanged using SHARE. A request to opt out will be treated as a request to withhold any use and disclosure of the individual's protected health information unless there is an emergency or disaster as described below. Participating Entities agree to approve such requests, subject to qualifications and limitations as described in the informational brochure referred to below or in these policies.

    1.1. Individuals shall be afforded the opportunity to exercise this choice periodically at the time of any service at a Participating Entity that is a health care provider or thereafter through a uniform opt-out process. This process will be fully developed by OHIT in its Privacy and Security Procedures.

    1.2. OHIT will, from time to time, furnish Participating Entities that are health care providers with an informational brochure about SHARE for distribution to individuals and for use in explaining the meaning and effect of participation or opting out. Participating Entities may customize the informational brochure as they deem appropriate to fit their circumstances. The brochure will also contain a link to the OHIT website where OHIT will provide an explanation of the meaning and effect of participation or opting out and a tool for opting out or revoking a prior opt-out election**.**

    1.3. The brochure shall explain the scope of an opt-out decision, the risks to the individual's data privacy and security if the individual participates, the effect and benefits of participation, and the effect and disadvantages of opting out. The brochure will explain that a Participating Entity's policies continue to govern access, use and disclosure in all other contexts.

    1.4. The brochure shall state that the Participating Entity (and other Participating Entities) will not withhold coverage or care from an individual on the basis of that individual's choice not to exchange his or her protected health information through SHARE or her included in SHARE.

    1.5. Participating Entities should furnish the brochure to individuals at the initiation of an episode of care and explain for individuals the opportunity to opt-out or ask questions. Each Participating Entity will have one or more

persons designated to answer questions about SHARE or about opting out or revoking a prior opt-out election.

1.6. Participating Entities may also direct individuals to the OHIT website and to a help line at OHIT where the individual can ask additional questions and obtain additional information about participation in OHIT and opt-out. OHIT as a business associate of the Participating Entities is authorized to provide information and answer individual questions about OHIT and the opt-out alternative on behalf of Participating Entities.

1.7. Participating Entities that are health plans provide only limited enrollment and eligibility information through SHARE and have limited or no face-to-face contact with individuals. Participating Entities that are health plans shall provide a description of SHARE, an explanation of the right to opt out, a link to the OHIT website and a phone number individuals can use to obtain additional information about SHARE, insurer access, and the right to opt out in their annual Notice and otherwise as they determine necessary.

1.8. An individual's election to opt out of participation in SHARE shall be communicated to OHIT in the manner provided by OHIT and be of System-wide effect once so communicated and processed. This means that once an individual has opted out of SHARE, no previously entered record will be made available other than as required by law or as permitted in an emergency or natural disaster. Individuals choosing to opt out may not have direct access to their Protected Health Information contained in SHARE as described in Policy 400, item 11.

2. **Change to Prior Election**. An individual may opt out or revoke a prior election to opt out at a later date as set out in the OHIT Privacy and Security Procedures. The brochure and information on the OHIT website should inform the individual that withdrawing a prior opt-out election will result in information that was previously unavailable through SHARE becoming available to all Participating Entities using SHARE.

3. **Effect of Choice.** An individual who opts out of SHARE opts out as to all of his or her records made available through SHARE, not just with respect to a particular Participating Entity or episode of care. The effect is System-wide. An individual's election to opt out, whether made at the time of service or subsequently, will have prospective effect only and will not impact access, use and disclosure occurring before the decision is received and communicated through SHARE.

4. **Limited Effect of Opt-Out**. A decision to opt out only affects the availability of the individual's protected health information through SHARE. Each Participating Entity's policies continue to govern access, use and disclosure in all other contexts and via all other media. Although an individual may opt-out, in the event of an emergency or

disaster their protected health information may be made available through SHARE as described in the OHIT Privacy and Security Procedures.

5. **Documentation.** Each Participating Entity shall document and maintain documentation that information about SHARE and about the ability to opt out of SHARE has been provided to the Participating Entity.

6. **Participating Entity's Choice.** Participating Entities shall develop and implement the necessary processes to allow an individual to choose not to have information about him or her included in SHARE. The uniform processes described in this Policy are not exclusive, and Participating Entities may adopt additional, not inconsistent, mechanisms.

7. **Provision of Coverage or Care.** A Participating Entity shall not withhold coverage or care from an individual on the basis of that individual's choice to opt out.

8. **Reliance.** Participating Entities will be entitled to assume that an individual has not opted-out if the individual's protected health information is available through SHARE.

OHIT Privacy
Policy 400: Access to and Use and Disclosure of Information

Scope and Applicability: This Policy applies to OHIT and all Participating Entities.

Policy:

1. **Compliance with Law.** Participating Entities shall access, use and disclose protected health information through SHARE only in a manner consistent with all applicable federal, state, and local laws and regulations and not for any unlawful or discriminatory purpose.

2. **Documentation and Reliance**. If applicable law requires that certain documentation exist or that other conditions be met prior to disclosing protected health information for a particular purpose, the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions. Each access and use of protected health information by a Participating Entity is a representation to every other Participating Entity whose protected health information is being accessed and used that all prerequisites under state and federal law for such disclosure by the disclosing Participating Entity have been met.[6]

3. **Purposes.** During its initial phase, a Participating Entity may request and use protected health information through SHARE only for the Participating Entity's treatment and payment purposes or for public health reporting purposes, and only to the extent necessary and permitted by applicable federal, state, and local laws and regulations and these Policies.[7] A Participating Entity may request and use protected health information through SHARE only if the Participating Entity has or has had the requisite relationship to the individual whose protected health information is being accessed and used.

4. **Prohibitions**. Information may not be requested for marketing or marketing related purposes without specific patient authorization. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participating Entity may not request or access information through SHARE.

5. **Participating Entity Policies.** Participating Entity uses and disclosures of, and requests for, protected health information through SHARE shall comply with OHIT's policies on Minimum Necessary and Information Subject to Special Protection.[8]

6. **Participating Entity Policies.** Each Participating Entity shall reference and maintain compliance with its own internal policies and procedures regarding

[6] See 45 C.F.R. § 164.530(j).
[7] 45 C.F.R. § 164.502(a), (b).
[8] 45 C.F.R. § 164.502(b).

disclosures of protected health information and the conditions that shall be met and documentation that must be obtained, if any, prior to making such disclosures.

7. **Subsequent Use and Disclosure.** A Participating Entity that has accessed information through SHARE and merged the information into its own record shall treat the merged information as part of its own record and thereafter use and disclose the merged information only in a manner consistent with its own information privacy policies and laws and regulations applicable to its own record. A Participating Entity shall not access protected health information through SHARE for the purpose of disclosing that information to third parties, other than for the Participating Entity's qualifying treatment and payment purposes.

8. **Accounting of Disclosures.** Each Participating Entity shall be responsible to account only for its own disclosures. OHIT shall provide a means by which each Participating Entity requesting information will indicate the purpose and use for such request so that Participating Entities that disclose information may document the purposes for which they have made disclosures for use in an accounting as required by HIPAA.[9] Unless a Participating Entity requesting information notes otherwise: (i) each request by a Participating Entity that is a provider is deemed to be for such Participating Entity's treatment purposes, (ii) each request by a Participating Entity that is a health plan is deemed to be for such Participating Entity's payment purposes, and (iii) each request by a Participating Entity that is acting as a plan administrator of one or more other health plans covered by HIPAA is deemed to be for the payment purposes of such other health plans. Each Participating Entity requesting information shall provide information required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement.

9. **Audit Logs.** Participating Entities and OHIT shall develop an audit log capability to document which Participating Entities posted and accessed the information about an individual through SHARE and when such information was posted and accessed.[10]

10. **Authentication.** OHIT shall follow a uniform authentication process for verifying and authenticating the identity and authority of each authorized user and Participating Entity.[11] [12] Individuals whose identities and authority have been authenticated by this process are referred to in these policies as an “authorized users.” Participating Entities shall be entitled to rely on SHARE’s user access and authorization safeguards and may assume an authorized user making a request for protected health information on behalf of a Participating Entity is authorized to do so. This process is described in greater detail in the OHIT Security Policies.

---

[9] 45 C.F.R. § 164.528.
[10] See 45 C.F.R. §§ 164.316, 164.308(a) (1) (i).
[11] See 45 C.F.R. §§ 164.514(h), 164.312(d).
[12] See **Connecting for Health**, "Authentication of System Users."

11. **Access.** Each Participating Entity should have a formal process through which it permits individuals to view their Protected Health Information that has been posted by the Participating Entity to SHARE.[13] Participating Entities and OHIT shall consider and work towards providing patients direct access to their Protected Health Information contained in SHARE.[14] This capability will not be available at the SHARE launch date.

12. **Application to BAs and Contractors.** Participating Entities shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

[13] See 45 C.F.R. § 164.524.
[14] See **Connecting for Health**, "Patients' Access to Their Own Health Information."

OHIT Privacy
Policy 500: Information Subject to Special Protection

Scope and Applicability: This Policy applies to OHIT and all Participating Entities.

Policy:

1. **Special Protection.** The operation of SHARE and these policies are intended to comply with the HIPAA Privacy Standards. The disclosure and use of some health information may be prohibited by special protections under federal, state, and/or local laws and regulations. Other health information may be deemed so sensitive that a Participating Entity has made special provision to safeguard the information, even if not legally required to do so. Each Participating Entity shall be responsible to identify what information is prohibited from use or disclosure under applicable law and what information (if any) is subject to special protection under that Participating Entity's policies, prior to disclosing any information through SHARE. **Participating Entities should not make protected health information requiring special protection available to SHARE.** Each Participating Entity is responsible for complying with laws and regulations and its own policies prior to disclosing this information on SHARE.

2. **Information Not Furnished.** For SHARE to be useful, the Participating Entities accessing health records must know if a patient's health record is complete or whether certain information has been withheld due to more stringent state and federal laws or Participating Entity policies.

1.1. Accordingly, Participating Entities accessing and using another Participating Entity's information obtained through SHARE should assume that the information made available **does not include any of the following**:

(a) Alcohol and substance abuse treatment program records; 42 CFR Part 2

(b) Records of predictive genetic testing performed for genetic counseling purposes; GINA

(c) Certain records of minors if under state law only the minor's consent to treatment is needed, the minor has consented to the care, but the minor is not the party electing not to opt out. In Arkansas, this may include the following records:

- Diagnosis and treatment of suspected abuse by a parent, guardian or personal representative;

1.2. This list is suggestive only. Other records may be added to the list. Participating Entities should assume the above listed records **are not included in SHARE.**

2. **Application to Business Associates and Contractors.** Participating Entities shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

OHIT Privacy
Policy 600: Minimum Necessary

Scope and Applicability: This Policy applies to OHIT, all Participating Entities and their BAs and contractors.

Policy:

1. **Requests.** Each Participating Entity shall request only the minimum amount of health information through SHARE as is necessary for the intended purpose of the request.

2. **Disclosures.** A Participating Entity may rely on the scope of a requesting Participating Entity's request for information as being consistent with the requesting Participating Entity's minimum necessary policy and needs.

3. **Workforce, BAs and Contractors**. Each Participating Entity shall adopt and apply policies to limit access to SHARE to members of its workforce who qualify as authorized users and only to the extent needed by such authorized users to perform their job functions or duties for the Participating Entity.

4. **Entire Medical Record.** A Participating Entity shall not use, disclose, or request an individual's entire medical record unless necessary and justified to accomplish the specific purpose of the use, disclosure, or request.

5. **Application to Health Plans.** A Participating Entity that is a health plan shall access and use PHI of another Participating Entity only for "payment" purposes as defined in 42 C.F.R. § 164.501. Participating Entities that are health plans shall initiate a search through SHARE only: (i) to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; (ii) to obtain or provide reimbursement for the provision of health care; (iii) to determine eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (iv) to risk adjust amounts due based on enrollee health status and demographic characteristics; (v) for billing, claims management, collection activities, obtaining payment under a contract for reinsurance, including stop-loss insurance and excess of loss insurance, and related health care data processing; (vi) to review health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and (vii) for utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services. All Participating Entities shall access and use only the minimum information necessary when accessing and using information for payment purposes.

6. **Application to Providers and Treatment Purposes**. While this minimum necessary policy is not required by HIPAA for providers accessing, using and disclosing health information for treatment purposes, they are encouraged to follow it when consistent with treatment needs.

7. **Application to BAs and Contractors.** Participating Entities shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

OHIT Privacy
Policy 700: Workforce, Agents, and Contractors

Scope and Applicability: This Policy applies to OHIT and all Participating Entities and their BAs and contractors.

Policy:

1. **Participating Entity Responsibility**. Each Participating Entity is responsible to establish and enforce policies designed to comply with its responsibilities as a Covered Entity under HIPAA and a Participating Entity in SHARE, and to train and supervise its authorized users to the extent applicable to their job responsibilities.

2. **Authorized Users.** All authorized users, whether members of a Participating Entity's workforce or member of the workforce of a BA or contractor shall execute an individual user agreement and acknowledge familiarity with and acceptance of the terms and conditions on which their access authority is granted. This shall include familiarity with applicable privacy and security policies of the Participating Entity, BA, or contractor, as applicable. Participating Entities shall determine to what extent members of their workforce or the workforce of BAs and contractors require additional training on the Participating Entity's obligations under their participation agreement and these policies, and arrange for and document such training. OHIT shall have the authority under the Participation Agreement to suspend, limit or revoke access authority to SHARE for any authorized user or Participating Entity for violation of OHIT's privacy and security policies or any federal or state law.

3. **Access to System.** Each Participating Entity shall allow access to SHARE only by authorized users who have a legitimate need to use SHARE and release or obtain information through SHARE. No workforce member, agent, or contractor shall have access to SHARE, except as an authorized user on behalf of a Participating Entity and subject to the Participating Entity's privacy and security policies and procedures and the terms of the individual's user agreement.

4. **Discipline for Non-Compliance.** Each Participating Entity shall implement disciplinary policies to hold authorized users, BAs and contractors accountable for following the Participating Entity's policies and procedures and for ensuring that they do not use, disclose, or request health information except as permitted by these Policies.[15] Examples of disciplinary measures include verbal and written warnings, demotion, and termination and may provide for retraining in certain circumstances.

5. **Reporting of Non-Compliance.** Each Participating Entity shall have a procedure, and shall encourage all workforce members, BAs and contractors to report any non-compliance with the Participating Entity's policies or the policies

[15] 45 C.R.F. § 164.530(e).

applicable to authorized users.[16] Each Participating Entity also shall establish a mechanism for individuals whose health information is included in SHARE to report any non-compliance with these Policies or concerns about improper disclosures of protected health information.

6. **Enforcing BAAs and Contractor Agreements**. Each Participating Entity shall implement policies for its workforce, BAs, contractors, or other third parties to designate authorized users of SHARE. Participating Entities must adhere to the following: (i) authorized users shall be subject to these Policies when accessing, using or disclosing information through SHARE; (ii) authorized users may have their access suspended or terminated for violation of these Policies or other terms and conditions of the authorized user agreement; and (iii) BAs, contractors and agents may have their contract with the Participating Entity terminated for violation of these Policies or for failure to enforce these policies.

[16] See 45 C.F.R. § 164.530(a), (d).

OHIT Privacy
Policy 800: Amendment of Data

Scope and Applicability: This Policy applies to OHIT and all Participating Entities.

Policy:

1. **Accepting Amendments.** Each Participating Entity shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information.[17] If an individual requests and the Participating Entity accepts an amendment to the health information about the individual, the Participating Entity, assisted by OHIT, shall make reasonable efforts to inform other Participating Entities that accessed or received such information through SHARE of the amendment within a reasonable time. Only the Participating Entity responsible for the record being amended may accept an amendment. If one Participating Entity believes there is an error in the record of another Participating Entity, it shall contact the responsible Participating Entity.

2. **Application to BAs and Contractors.** Participating Entities shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

[17] 45 C.F.R. § 164.526.

OHIT Privacy
Policy 900: Requests for Restrictions

Scope and Applicability: This Policy applies to all Participating Entities.

Policy:

1. **Recipient Responsibility**. A Participating Entity, when accessing SHARE shall not be expected to know of or comply with a restriction on use or disclosure agreed to by a Participating Entity that provides data.

2. **Data Provider Responsibility**. If a Participating Entity agrees to an individual's request for restrictions,[18] as permitted under the HIPAA Privacy Rule, such Participating Entity shall ensure that it complies with the restrictions. This shall include not exchanging the individual's protected health information through SHARE, including opting the individual out of SHARE, if required by the restriction. Participating Entities should advise individuals that opting out only affects access, use and disclosure of their protected health information through SHARE. When evaluating a request for a restriction, the Participating Entity shall consider the implications that agreeing to the restriction would have on the accuracy, integrity and availability of information through SHARE.

[18] Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 45 C.F.R. § 164.522. For example, an individual could request that information not be used or disclosed for a particular purpose or that certain information not be disclosed to a particular individual. Covered entities are not required to agree to such requests under HIPAA.

OHIT Privacy
Policy 1000: Mitigation

Scope and Applicability: This Policy applies to OHIT, all Participating Entities and their BAs and contractors.

Policy:

1. **Duty to Mitigate**. Each Participating Entity shall implement a process to mitigate, and shall mitigate to the extent practicable, the harmful effects that are known to the Participating Entity of an access, use or disclosure of protected health information through SHARE that is in violation of applicable laws or regulations or these Policies and that is caused or contributed to by the Participating Entity or its workforce members, agents, and contractors. Steps to mitigate could include, but are not limited to, Participating Entity notification to the individual or Participating Entity request to the party who improperly received such information to return or destroy impermissibly disclosed information.

2. **Duty to Cooperate**. A Participating Entity that has caused or contributed to a privacy breach or that could assist with mitigation of the effects of a breach shall cooperate with OHIT and with another Participating Entity that has the primary obligation to mitigate a breach. This obligation exists whether the Participating Entity is directly responsible or whether the breach was caused or contributed to by members of the Participating Entity's workforce or by its BAs or contractor or their workforce.

3. **Notification to OHIT**. A Participating Entity primarily responsible to mitigate shall notify the OHIT compliance officer of all events requiring mitigation and of all actions taken to mitigate. OHIT may facilitate the mitigation process if asked. OHIT shall provide training on breach mitigation.

4. **Application to BAs and Contractors.** Participating Entities shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

OHIT Privacy
Policy 1100: Investigations; Incident Response System

Scope and Applicability: This Policy applies to OHIT, all Participating Entities and their BAs and contractors.

Policy:

1. **Duty to Investigate**. Each Participating Entity shall promptly investigate reported or suspected privacy breaches implicating privacy or security safeguards deployed by OHIT (or its contractors) according to its own policies. Upon learning of a reported or suspected breach, the Participating Entity shall notify OHIT within five business days and any other Participating Entity whom the notifying Participating Entity has reason to believe is affected or may have been the subject of unauthorized access, use or disclosure. OHIT shall participate in the investigation and remedial actions taken. OHIT need not be notified of specific workforce disciplinary actions. Each investigation shall be documented. At the conclusion of an investigation, a Participating Entity shall document its findings and any action taken in response to an investigation. A summary of the findings shall be sent to OHIT.

2. **Incident Response.** OHIT shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by Participating Entities or discovered by OHIT. The incident response system shall include the following features, each applicable as determined by the circumstances:

   2.1 Cooperation in any investigation conducted by the Participating Entity or direct investigation by OHIT;

   2.2 Notification of other Participating Entities or authorized users as needed to prevent further harm or to enlist cooperation in the investigation and/or mitigation of the breach;

   2.3 Cooperation in any mitigation steps initiated by the Participating Entity;

   2.4 Furnishing audit logs and other information helpful in the investigation;

   2.5 Developing and disseminating remediation plans to strengthen safeguards or hold Participating Entities or authorized users accountable;

   2.6 Any other steps mutually agreed to as appropriate under the circumstances; and

   2.7 Any other step required under the incident reporting and investigation system contained in the OHIT Security Policies.

3. **OHIT Cooperation**. OHIT shall cooperate with a Participating Entity in any investigation of the Participating Entity's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-

investigation by the Participating Entity, when the investigation implicates OHIT conduct, or the conduct of another Participating Entity or authorized user, or the adequacy or integrity of System safeguards.

4. **Participating Entity Cooperation**. Each Participating Entity shall cooperate with OHIT in any investigation of OHIT or of another Participating Entity into OHIT's or such other Participating Entity's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by OHIT or the other Participating Entity, when the investigation implicates such Participating Entity's compliance with OHIT policies or the adequacy or integrity of System safeguards.

5. **Application to BAs and Contractors.** Participating Entities shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

OHIT Privacy
Policy 1200: Authorized User Controls

Scope and Applicability: This Policy applies to OHIT, all Participating Entities and their BAs and contractors. This Policy is to be read and applied in conjunction with the OHIT Security Policy.

Policy:

1. Participating Entity Responsibilities. Each Participating Entity is responsible to:

1.1 Designate its responsible contact person who shall be initially responsible on behalf of the Participating Entity for compliance with these policies and to receive notice on behalf of the Participating Entity. For Participating Entities that have their own system administrator, this shall ordinarily be the SHARE administrator.

1.2 Designate its own authorized users from among its workforce, and designate BAs and contractors authorized to act as (or designate from among their workforce) authorized users on its behalf.

1.3 Train and supervise its authorized users and require any BA or contractor to train and supervise its authorized users consistent with the Participating Entity's and OHIT's privacy policies and with the terms of the Participating Entity's privacy policies and the BA Agreement as applicable.

1.4 In the case of Participating Entities with a System Administrator, immediately suspend, limit or revoke access authority upon a change in job responsibilities or employment status of an authorized user. Revocation shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participating Entity.

1.5 For Participating Entities without their own System Administrator, immediately notify OHIT or OHIT's designee of the change so that OHIT may revoke access authority. Notification shall occur prior to, contemporaneously with, or immediately following such a change so as to prohibit continued access authority for individuals who no longer need it on behalf of the Participating Entity.

1.6 Hold their authorized users accountable for compliance with OHIT and the Participating Entity's policies and, as applicable, the terms of any BA Agreement.

2. OHIT Responsibilities. OHIT or OHIT's designee is responsible to:

2.1 Grant access authority to individuals designated by a Participating Entity, subject to reserved authority to suspend, limit, or revoke such access authority as described later.

2.2 Train and supervise its own authorized users on these policies and the standard terms required by its BA Agreement with Participating Entities.

2.3 Suspend, limit or revoke access authority for its own authorized users or any authorized user who is a member of the workforce of any subcontractor of OHIT as required by these policies or the terms of its BA Agreement in the event of breach or non-compliance.

2.4 Immediately revoke access authority upon a change in job responsibilities or employment status of its own authorized users or the authorized user of its contractor.

2.5 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 Participating Entity's privacy policies, OHIT policies or the terms of the user agreement, if OHIT determines that doing so is necessary for the privacy of individuals or the security of SHARE.

2. **OHIT Security Policy**. The details of how to grant and revoke access authority are contained in the OHIT Privacy and Security Procedures.

3. **Application to BAs and Contractors.** Participating Entities shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.