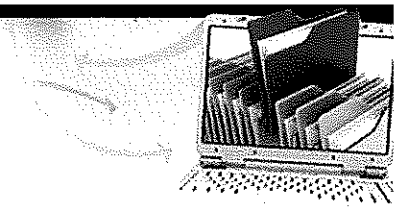
OHIT
Arkansas Office of Health Information Technology



ARKANSAS OFFICE OF HEALTH INFORMATION TECHNOLOGY (OHIT) PRIVACY POLICIES

TABLE OF CONTENTS

POLICY 100: COMPLIANCE WITH LAW AND POLICY..... 6

POLICY 200: NOTICE OF PRIVACY PRACTICES..... 8

POLICY 300: INDIVIDUAL CONTROL OF INFORMATION AVAILABLE THROUGH SHARE.....10

POLICY 400: ACCESS TO AND USE AND DISCLOSURE OF INFORMATION..... 11

POLICY 500: INFORMATION SUBJECT TO SPECIAL PROTECTION..... 13

POLICY 600: MINIMUM NECESSARY..... 14

POLICY 700: WORKFORCE, AGENTS, AND CONTRACTORS..... 16

POLICY 800: AMENDMENT OF DATA..... 18

POLICY 900: REQUESTS FOR RESTRICTIONS 19

POLICY 1000: MITIGATION 20

POLICY 1100: INVESTIGATIONS; INCIDENT RESPONSE SYSTEM..... 21

POLICY 1200: AUTHORIZED USER CONTROLS..... 23

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 C.F.R. § 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. Openness about developments, procedures, policies, technology and practices with respect to the treatment of personal health data is essential 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 exercise reasonable control over that information. This transparency helps promote privacy practices and instills confidence with regard to data privacy, which in turn can help increase consumer participation in health information networks.

Purpose Specification and Minimization. Data use must be limited to the amount necessary to accomplish specified purposes. Minimization of use will help reduce privacy violations, which can easily occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

Collection Limitation. Personal health data should be obtained only by fair and lawful means, and, if applicable, with the knowledge or consent of the pertinent individual. In an electronic networked environment, it is particularly important for individuals to understand how information concerning them is being collected because electronic collection methods may be confusing to average users. Similarly, individuals may not be aware of the potential abuses that can arise if they submit personal health information via an electronic method.

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, payment or operations purposes of the requesting Participating Entity or for other purposes permitted by law. The use and disclosure of health information should be limited to those purposes specified by SHARE. Certain exceptions such as public health reporting, law enforcement or security may warrant reuse of data for other purposes. However, when data is used for purposes other than those originally specified, prior de-identification of the data can

help protect individual privacy while enabling important benefits to be derived from the information.

Individual Participation and Control. Every individual should retain the right to request and receive in a timely and intelligible manner information regarding who has that individual's health data and what specific data the party has, to know any reason for a denial of such request, and to challenge or amend any personal information. Because individuals have a vital stake in their own personal health information, such rights enable them to be participants in the collection and use of their data. Individual participation promotes data quality, privacy, and confidence in privacy practices.

Data Integrity and Quality. Health data should be accurate, complete, relevant and up-to-date to ensure its usefulness. The quality of health care depends on the existence of accurate health information. Moreover, individuals can be adversely affected by inaccurate health information in other arenas, such as insurance and employment. Therefore, SHARE must maintain the integrity of health data 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. Security safeguards are essential to privacy protection because they help prevent data loss, corruption, unauthorized use, modification, and disclosure. With increasing levels of cyber-crime, networked environments may be particularly susceptible without adequate security controls. Design and implementation of various technical security precautions such as identity management tools, data scrubbing, hashing, auditing, authenticating, and other tools can strengthen information privacy.

Accountability and Oversight. Privacy protections have little weight if privacy violators are not held accountable for compliance failures. Employee training, privacy audits, and other oversight tools can help to identify and address privacy violations and security violations and security breaches by holding accountable those who violate privacy requirements, and by identifying and correcting weaknesses in their security systems.

Remedies. The maintenance of privacy protection depends upon legal and financial means to remedy any privacy or security breaches. Such remedies should hold violators accountable for compliance failures, reassure individuals about the organization's commitment to information privacy, and mitigate any harm that privacy violations may cause individuals.

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 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.

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 shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. Each Participating Entity shall use reasonable efforts to stay up-to-date of any changes or updates to and interpretations of such laws and regulations to ensure compliance.[2]

2. OHIT Policies. Each Participating Entity shall, at all times, comply with these OHIT Policies ("OHIT Policies"). These OHIT Policies may be revised and updated from time to time. 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 by posting the updated policy on the OHIT website. 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 ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and these OHIT Policies. In the event of a conflict between these OHIT Policies and an institution's own policies and procedures, the Participating Entity shall comply with the policy that is more protective of individual privacy and security.

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

[2] 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.

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") that complies with applicable law and this Policy. 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[3] and comply with applicable laws and regulations. The Notice also shall include a description of SHARE, and inform individuals regarding: (1) what information the institution may include in and make available through SHARE; (2) who is able to access the information available in SHARE; (3) for what purposes such information can be accessed; and (4) how the individual can have his or her information removed from 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 SHARE, an electronic health information exchange, to other health care providers and health plans that request your information for their treatment, payment, operations and public health reporting purposes. Participation in an electronic health information exchange also lets us see their information about you for our treatment, payment and operations purposes or for public health reporting. As a patient, you must 'opt out', if you choose not to have information about you made available through SHARE. "

2. Provision to Individuals. Each Participating Entity shall have its own policies and procedures governing distribution of the Notice to individuals, which policies and procedures shall be consistent with this policy and comply with applicable laws and regulations.

- For Participating Entities that are health care providers, the Notice shall be: (1) available to the public upon request; (2) posted on all web sites of the Participating Entity and available electronically through such sites; (3) provided to a patient at the date of first service delivery; (4) available at the institution; and (5) posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.[4]
- For Participating Entities that are health plans, the Notice shall be: (1) available to the public upon request; (2) provided to new enrollees at the time of plan enrollment; (3) provided to current plan enrollees within 60 days of a material revision; and posted on the plan's web sites and available electronically through such sites. Participating health plan institutions also shall notify individuals covered by the plan of the availability of the Notice and how to obtain a copy at least once every three years. [5]

[3] 45 C.F.R. § 164.520 (b).
[4] 45 C.F.R. § 164.520 (c)(2),(3)
[5] 45 C.F.R. § 164.520 (c)(1),(3)

3. Individual Acknowledgement. Each Participating Entity that is a health care provider shall make a good faith effort to obtain the individual's written acknowledgement of receipt of the Notice or to document their efforts and/or failure to do so. The acknowledgement of the Notice shall comply with all applicable laws and regulations.[6] Each Participating Entity shall have its own policies and procedures governing obtaining an acknowledgement, which policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

4. Participating Entity Choice. Participating Entities may choose a more proactive notice distribution process than provided herein and may include more detail in their Notice of Privacy Practices. Possible additional protections for individuals whose information may be made available through SHARE (not all of which pertain to notice policies alone) could include: mailing the revised notice or a notification letter allowing for removal or exclusion of the information about that individual from SHARE to every individual prior to loading the information into SHARE or shortly thereafter; loading individual information into SHARE on a going-forward, new individual encounter basis only; developing a method for time-stamping a SHARE records to indicate when the record was loaded into the index;

[6] 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 Not to Have Information Included in SHARE.** All individuals may choose not to have information about them made available through SHARE.

2. **Effect of Choice.** An individual's choice not to have information about him or her included in or made available through SHARE shall be exercised through the Participating Entity, as described in the institution's Notice, after which time the institution shall no longer make the individual's information available through SHARE.

3. **Limited Effect of Choice.** 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 disclosures 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.

4. **Revocation.** An individual who has chosen not to make information concerning him or her available through SHARE subsequently may be included in SHARE only if the individual revokes his or her decision or subsequently chooses to renew participation in SHARE.

5. **Documentation.** Each Participating Entity shall document and maintain documentation or all patients' decisions not to have information about them included in SHARE.

6. **Participant Choice.** Participating Entities shall establish reasonable and appropriate processes to enable the exercise of a patient's choice not to have information about him or her included in SHARE. Each Participating Entity retains the authority to decide the process by which to obtain patient consent prior to making information available through SHARE.

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 not to have information about him or her included in SHARE.

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. All disclosures of Protected Health Information through SHARE and the use of information obtained through SHARE shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing Protected Health Information for a particular purpose, the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing institution.[7]

2. Reliance. 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.

3. Purposes. A Participating Entity may request health information through SHARE only for purposes permitted by applicable law. Each Participating Entity shall provide or request health information through SHARE only to the extent necessary and only for those purposes that are permitted by applicable federal, state and local laws and regulations and these Policies.[8] Information may not be requested for 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 information through SHARE.

4. OHIT Policies. Uses and disclosures of and requests for Protected Health Information via SHARE shall comply with all OHIT Policies, including, but not limited to, the OHIT Policy on Minimum Necessary and the OHIT Policy on Information Subject to Special Protection.[9]

5. Participating Entity Policies. Each Participating Entity shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.

[7] See 45 C.F.R. § 164.530(j).
[8] 45 C.F.R. § 164.502(a),(b).
[9] 45 C.F.R. § 164.502(b).

6. Accounting of Disclosures. Each Participating Entity disclosing Protected Health Information through SHARE shall work toward implementing a system to document the purposes for which such disclosures are made, as provided by the requesting institution, and any other information that may be necessary for compliance with the HIPAA Privacy Rule's accounting of disclosures requirement.[10] Each Participant is responsible for ensuring its compliance with such requirement and may choose to provide individuals with more information in the accounting than is required. Each requesting institution shall provide information required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement.

7. 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.[11]

8. Authentication. OHIT shall follow a uniform authentication process for verifying and authenticating the identity and authority of each authorized user and Participating Entity.[12, 13] Individuals whose identities and authority have been authenticated by this process are referred to in these policies as "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 and Security Framework.

9. 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.

[10] See 45 C.F.R. § 164.528. For HIPAA Covered Entities, this is currently required by law.
[11] See 45 C.F.R. § 164.316, 164.308(a)(1)(i)
[12] 45 C.F.R. §§ 164.514(h), 164.312(d).
[13] See ***Connecting for Health,*** *"Authentication of System Users."*

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. Some health information may be subject to special protection under federal, state, and/or local laws and regulations. Each Participating Entity shall determine and identify what information is subject to special protection under applicable law prior to disclosing any information through SHARE. Each Participating Entity is responsible for complying with such laws and regulations. **Participating Entities should not make Protected Health Information requiring special protection available to 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.

2.1 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; See 42 CFR Part 2

(b) Records of predictive genetic testing performed for genetic counseling purposes; See The Genetic Information Nondiscrimination Act of 2008 (Pub.L. 110–233, 122 Stat. 881, enacted May 21, 2008

(c) Certain records of minors including the following: diagnosis and treatment of suspected abuse by a parent, guardian or personal representative;

2.2. 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. The Minimum Necessary Policy does not apply to requests by health care providers for treatment purposes.

2. Uses and Disclosures. Each Participating Entity shall use and disclose only the minimum amount of health information obtained through SHARE as is necessary for the purpose of each use or disclosure. Each Participating Entity shall share health information obtained SHARE with and allow access to such information by only those workforce members, agents, and contractors who need the information in connection with their job functions or duties. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

4. 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 except where justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request. This limit does not apply to disclosures to or requests by a health care provider for treatment purposes or disclosures required by law.

5. Application to Providers for 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.

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 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 those workforce members, agents, and contractors who have a legitimate and appropriate need to use SHARE and/or release or obtain information through SHARE. No workforce member, agent, or contractor shall be provided with access to SHARE without first having been trained on these Policies, as set forth below.

4. Training. Each Participating Entity shall develop and implement a training program for its workforce members, agents, and contractors who will have access to SHARE to ensure compliance with these Policies.[14] The training shall include a detailed review of applicable Policies and each trained workforce member, agent and contractor shall sign a representation that he or she received, read and understands these Policies.

4. Discipline for Non-Compliance. Each Participating Entity shall implement procedures to discipline and hold workforce members, agents, and contractors accountable for ensuring that they do not use, disclose or request health information except as permitted by these Policies and that they comply with these Policies.[15] Such discipline measures shall include, but not be limited to, verbal and written warnings, demotion, and termination and provide for retraining where appropriate.

[14] Sec 45 C. F. R. § 164.530(b).
[15] 45 C. F. R. § 164.530 (e).

5. Reporting of Non-Compliance. Each Participating Entity shall have a mechanism for, and shall encourage, all workforce members, agents, and contractors to report any non-compliance with these Policies to the Participating Entity.[16] Each Participating Entity also shall establish a process for individuals whose health information is included in SHARE to report any non-compliance with these Policies or concerns about improper disclosures of information about them.

6. Enforcing BAAs and Contractor Agreements. Each Participating Entity shall require in any relationship with a Business Associate, contractor, or other third party (which may include staff physicians) that will result in such third party becoming an authorized user on behalf of the Participating Entity, or that will result in members of the workforce of such third party becoming an authorized user on behalf of the Participant, that: (i) such third party and any member of its workforce shall be subject to these Policies when accessing, using or disclosing information through the System; (ii) that such third parties and/or authorized users on its workforce may have their access suspended or terminated for violation of these Policies or other terms and conditions of the authorized user agreement; and (iii) that such third party may have its contract with the Participant terminated for violation of these Policies or for failure to enforce these policies among its workforce.

[16] 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 the amendment of health information. [17, 18] If an individual or treating physician requests, and the Participating Entity accepts, an amendment to the health information, 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, if the recipient institution may have relied or could foreseeably rely on the information to the detriment of the individual. 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.
[18] Arkansas Hospital **RULES AND REGULATIONS FOR HOSPITALS AND RELATED INSTITUTIONS IN ARKANSAS 2007, Section 14.** See : **http://www.healthy.arkansas.gov/aboutADH/RulesRegs/Hospitals.pdf** 14-1

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,[19] as permitted under the HIPAA Privacy Rule, such Participating Entity shall ensure that it complies with the restrictions when releasing information through SHARE. This shall include not exchanging the individual's Protected Health Information through SHARE and 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. If an agreed-upon restriction will or could affect the requesting institution's uses and/or disclosures of health information, at the time of disclosure, the Participant disclosing such health information shall notify the requesting institution of the fact that certain information has been restricted, without disclosing the content of any such restriction. 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.

[19] 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.

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 and take appropriate remedial action, any harmful effect that is known to the Participating Entity of a use or disclosure of Protected Health Information through SHARE that is in violation of applicable laws and/or regulations and/or these Policies by the Participating Entity or its workforce members, agents, and contractors. Steps to mitigate could include, among other things, Participating Entity notification to the individual of the disclosure of information about them, 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 Privacy 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. Individual Complaints. Any individual may submit a complaint about a use or disclosure of Protected Health Information by OHIT to either OHIT or the Secretary of the Department of Health and Human Services (HHS) in Washington, DC. If the individual wants to file a formal complaint with OHIT, he or she should be directed to the OHIT Privacy Officer. If the individual wants to file his/her complaint with the Secretary of HHS, he/she should be directed to the Office for Civil Rights website (www.hhs.gov/ocr/hipaa). The OHIT Privacy Officer will document each privacy complaint received including in the documentation a brief description of and/or the basis for the complaint.

The Privacy Officer will supplement the initial documentation to include documentation of the investigation and any actions taken in response to the complaint. All documentation relating to the individual's complaint will be maintained for a minimum of six (6) years.

2. 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.

3. Compliance with HIPAA Security Rule. OHIT will comply with the HIPAA Security Rule. Each Participating Entity will be required to comply with all applicable federal, state and local laws, which may include laws relating to notification of patients.

4. Training and Enforcement. Each Participating Entity that may have access to patient data via SHARE must appropriately train its personnel and inform them that any breach of confidentiality is actionable. Each Participating Entity should follow and enforce its own confidentiality policies and disciplinary procedures.

5. Notification of Breach. As a Business Associate, OHIT must report any breaches and/or security incidents to the particular data provider whose data was improperly used. Each Participating Entity must agree to inform OHIT of any breach of confidentiality.

6. Incident Response. OHIT shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by a Participating Entity or discovered

by OHIT. The incident response system shall include the following features, each applicable as determined by the circumstances:

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

6.2 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;

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

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

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

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

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

7. 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.

8. 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.

9. 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 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 the OHIT Security Officer 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 Procedures. The details of how to grant and revoke access authority are contained in the OHIT Security Framework.

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.