Title 25. State Government

Chapter V. Office of Health Information Technology

Subchapter A. Generally

Part 20. Arkansas Office of Health Information Technology Privacy Policies

Codification Notes. This part, as originally promulgated prior to the codification of the Code of Arkansas Rules, provided as follows: "Arkansas Office of Health Information Technology (OHIT) Privacy Policies".

This part, as originally promulgated prior to the codification of the Code of Arkansas Rules of 2024, provided as follows: "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."

Subpart 1. Generally

25 CAR § 20-101. Definitions.

The following terms used throughout this rule are defined as follows:

(1)(A) "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:

(i) Claims processing or administration;

(ii) Data analysis, processing, or administration;

(iii) Utilization review;

(iv) Quality assurance;

(v) Billing;

(vi) Benefit management;

(vii) Practice management and repricing; or

(viii) Any other function or activity;

(B) See 45 C.F.R. § 160.103;

(2) "Individual" means those persons whose protected health information is transmitted using the State Health Alliance for Records Exchange;

(3)(A) "Office of Health Information Technology" is a business associate of the participating entities who are covered entities under HIPAA.

(B) The Office of Health Information Technology 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; and

(4)(A) "Participating entities" means those entities which provide data to the State Health Alliance for Records Exchange and those entities which obtain and use data from the State Health Alliance for Records Exchange as health care providers, health plans, or health care clearinghouses, collectively "covered entities" as defined by HIPAA.

(B) All participating entities are covered entities under HIPAA or have signed participation agreements with the Office of Health Information Technology.

(C) Participating entities should not be confused with "individuals" whose protected health information is exchanged using the State Health Alliance for Records Exchange.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. This part, as promulgated prior to codification as the Code of Arkansas Rules, contained a footnote to 25 CAR § 20-101(4) as follows: "45 C.F.R. § 160.103".

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L.

No. 104-191.

25 CAR § 20-102. Privacy principles.

(a) These Office of Health Information Technology Privacy Policies, are rooted in nine (9) 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 the office that, taken together with privacy policies and procedures already deployed by participating entities as covered entities under HIPAA from a comprehensive array of administrative safeguards addressing privacy of protected health information.

(b) The office 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 the State Health Alliance for Records Exchange, and State Health Alliance for Records Exchange's unique operating environment.

(c) 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 healthcare system.

(d)(1) 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.

(2) The guiding office privacy principles are as follows:

(A) **Openness and transparency.**

(i) Openness about developments, procedures, policies, technology, and practices with respect to the treatment of personal health data is essential to protecting privacy.

(ii) 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.

(iii) 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;

(B) **Purpose specification and minimization.**

(i) Data use must be limited to the amount necessary to accomplish specified purposes.

(ii) Minimization of use will help reduce privacy violations, which can easily occur when data is collected for one (1) legitimate reason and then reused for different or unauthorized purposes;

(C) **Collection limitation.**

(i) Personal health data should be obtained only by fair and lawful means, and, if applicable, with the knowledge or consent of the pertinent individual.

(ii) 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.

(iii) Similarly, individuals may not be aware of the potential abuses that can arise if they submit personal health information via an electronic method;

(D) **Use limitation.**

(i) Protected health information should be obtained by one (1) 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.

(ii) The use and disclosure of health information should be limited to those purposes specified by the State Health Alliance for Records Exchange.

(iii) Certain exceptions such as public health reporting, law enforcement, or security may warrant reuse of data for other purposes.

(iv) However, when data is used for purposes other than those originally specified, prior deidentification of the data can help protect individual privacy while enabling important benefits to be derived from the information;

(E) **Individual participation and control.**

(i) Every individual should retain the right to:

(a) 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;

(b) Know any reason for a denial of such request; and

(c) Challenge or amend any personal information.

(ii) 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.

(iii) Individual participation promotes data quality, privacy, and confidence in privacy practices;

(F) **Data integrity and quality.**

(i) Health data should be accurate, complete, relevant, and up-to-date to ensure its usefulness.

(ii) The quality of health care depends on the existence of accurate health information.

(iii) Moreover, individuals can be adversely affected by inaccurate health information in other arenas, such as insurance and employment.

(iv) Therefore, the State Health Alliance for Records Exchange 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;

(G) **Security safeguards and controls.**

(i) Security safeguards are essential to privacy protection because they help prevent data loss, corruption, unauthorized use, modification, and disclosure.

(ii) With increasing levels of cybercrime, networked environments may be particularly susceptible without adequate security controls.

(iii) 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;

(H) **Accountability and oversight.**

(i) Privacy protections have little weight if privacy violators are not held accountable for compliance failures.

(ii) Employee training, privacy audits, and other oversight tools can help to identify and address privacy violations, security violations, and security breaches by holding accountable those who violate privacy requirements, and by identifying and correcting weaknesses in their security systems;

(I) **Remedies.**

(i) The maintenance of privacy protection depends upon legal and financial means to remedy any privacy or security breaches.

(ii) Such remedies should:

(a) Hold violators accountable for compliance failures;

(b) Reassure individuals about the organization's commitment to information privacy; and

(c) Mitigate any harm that privacy violations may cause individuals; and

(J) **Reliance on covered entity policies and enforcement.**

(i) While the office should have a number of core policies and procedures for the benefit and confidence of all participating entities, the office should not try to replace policies, procedures, and methods already adopted by participating entities as covered entities under HIPAA.

(ii) The office 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.

(iii) The office policies incorporate the principles outlined in the preceding principles as well as basic requirements set forth in HIPAA.

(iv) The office policies seek to achieve a balance between maintaining the confidentiality of health information and maximizing the benefits of such information.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

25 CAR § 20-103. Compliance with law and policy.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology and all participating entities.

(b) **Laws.** Each participating entity shall:

(1) 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; and

(2) Use reasonable efforts to stay up-to-date on any changes or updates to and interpretations of such laws and regulations to ensure compliance.

(c) **Office policies.**

(1) Each participating entity shall, at all times, comply with these office policies, or "Office of Health Information Technology Policies".

(2) These office policies may be revised and updated from time to time.

(3) Amendments shall be effective when adopted by the office with review by the State Health Alliance for Records Exchange Health Information Exchange Council and promulgated as required by the Arkansas Administrative Procedure Act, Arkansas Code § 25-15-201 et seq.

(4) The office shall notify participating entities of all policy changes by posting the updated policy on the office website.

(5) Each participating entity is responsible for ensuring it has, and is in compliance with, the most recent version of these office policies.

(d) **Participating entity policies.**

(1) Each participating entity is responsible for ensuring that it has the

requisite, appropriate, and necessary internal policies for compliance with applicable laws and these office policies.

(2) In the event of a conflict between these office 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.

(e) **Participating entity criteria.**

(1)(A) Each participating entity shall itself be a HIPAA covered entity or have executed a participation agreement with the State Health Alliance for Records Exchange.

(B) 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.

(2) Each participating entity must commit to be a data provider to the extent possible in order to become a data user.

(f) **User criteria.**

(1) Authorized users are individuals who have been granted access authority.

(2)(A) Each authorized user derives his or her permission to access and use the State Health Alliance for Records Exchange from a participating entity.

(B) Therefore, each authorized user must maintain a current relationship to a participating entity in order to use the State Health Alliance for Records Exchange.

(C) Authorized users must therefore be:

(i) Participating entities, such as 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.

(3) 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.

(g) **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 BA agreements.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. This section, as promulgated prior to the codification of the Code of Arkansas Rules provided a footnote to 25 CAR § 20-104(b)(2) as follows: "The participants acknowledge the need to revise policies and contain other technical and administrative features to conform to HITECH and regulations to be promulgated thereunder".

"HITECH" means the Health Information Technology for Economic and Clinical Health Act, which was enacted as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5.

25 CAR § 20-104. Notice of privacy practices.

(a) **Scope and applicability.**

(1) This policy applies to all participating entities.

(2)(A) Each participating entity that is a covered entity under HIPAA shall develop and maintain a notice of privacy practices, known as "notice", that complies with applicable law and this policy.

(B) The notice must describe the uses and disclosures of protected health information contemplated through the participating entity's participation in the State Health Alliance for Records Exchange.

(b) **Content.**

(1) The notice must meet the content requirements set forth under the HIPAA privacy rule and comply with applicable laws and regulations.

(2) The notice also shall include a description of the State Health Alliance for Records Exchange and inform individuals regarding:

(A) What information the institution may include in and make available through the State Health Alliance for Records Exchange;

(B) Who is able to access the information available in the State Health Alliance for Records Exchange;

(C) For what purposes such information can be accessed; and

(D) How the individual can have his or her information removed from the State Health Alliance for Records Exchange.

(3) The Office of Health Information Technology 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."

(c) **Provision to individuals.**

(1) 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.

(2) For participating entities that are healthcare providers, the notice shall be:

(A) Available to the public upon request;

(B) Posted on all websites of the participating entity and available electronically through such sites;

(C) Provided to a patient at the date of first service delivery;

(D) Available at the institution; and

(E) Posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the notice.

(3) For participating entities that are health plans, the notice shall be:

(A) Available to the public upon request;

(B) Provided to new enrollees at the time of plan enrollment;

(C) Provided to current plan enrollees within sixty (60) days of a material revision; and

(D) Posted on the plan's websites and available electronically through such sites.

(4) 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 (3) years.

(d) **Individual acknowledgement.**

(1) Each participating entity that is a healthcare 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.

(2) The acknowledgement of the notice shall comply with all applicable laws and regulations.

(3) 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.

(e) **Participating entity choice.**

(1) Participating entities may choose a more proactive notice distribution process than provided herein and may include more detail in their notice of privacy practices.

(2) Possible additional protections for individuals whose information may be made available through the State Health Alliance for Records Exchange, not all of which pertain to notice policies alone, could include:

(A) Mailing the revised notice or a notification letter allowing for removal

or exclusion of the information about that individual from the State Health Alliance for Records Exchange to every individual prior to loading the information into the State Health Alliance for Records Exchange or shortly thereafter;

(B) Loading individual information into the State Health Alliance for Records Exchange on a going-forward, new individual encounter basis only; or

(C) Developing a method for time-stamping State Health Alliance for Records Exchange records to indicate when the record was loaded into the index.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. This section, as promulgated prior to the codification of the Code of Arkansas Rules, provided a footnote to 25 CAR § 20-105(b)(1) as follows: "45 C.F.R. § 164.520 (b)".

This section, as promulgated prior to the codification of the Code of Arkansas Rules, provided a footnote to 25 CAR § 20-105(c)(1)(E) as follows: "45 C.F.R. § 164.520 (c)(2),(3)".

This section, as promulgated prior to the codification of the Code of Arkansas Rules, provided a footnote to 25 CAR § 20-105(c)(4) as follows: "45 C.F.R. § 164.520 (c)(1),(3)".

This section, as promulgated prior to the codification of the Code of Arkansas Rules, provided a footnote to 25 CAR § 20-105(d)(2) as follows: "45 C.F.R. § 164.520 (c)(2)(ii)".

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

"SHARE" means the State Health Alliance for Records Exchange.

25 CAR § 20-105. Individual control of information available through the State Health Alliance for Records Exchange.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology, the State Health Alliance for Records Exchange, and all participating entities.

(b) **Choice not to have information included in the State Health Alliance for Records Exchange.** All individuals may choose not to have information about them made available through the State Health Alliance for Records Exchange.

(c) **Effect of choice.** An individual's choice not to have information about him or her included in or made available through the State Health Alliance for Records Exchange 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 the State Health Alliance for Records Exchange.

(d) **Limited effect of choice.**

(1) A decision to opt out only affects the availability of the individual's protected health information through the State Health Alliance for Records Exchange.

(2) Each participating entity’s policies continue to govern access, use, and disclosures in all other contexts and via all other media.

(3) Although an individual may opt out, in the event of an emergency or disaster their protected health information may be made available through the State Health Alliance for Records Exchange.

(e) **Revocation.** An individual who has chosen not to make information concerning him or her available through the State Health Alliance for Records Exchange subsequently may be included in the State Health Alliance for Records Exchange only if the individual revokes his or her decision or subsequently chooses to renew participation in the State Health Alliance for Records Exchange.

(f) **Documentation.** Each participating entity shall document and maintain documentation of all patients' decisions not to have information about them included in the State Health Alliance for Records Exchange.

(g) **Participant choice.**

(1) 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 the State Health Alliance for Records Exchange.

(2) Each participating entity retains the authority to decide the process by which to obtain patient consent prior to making information available through the State Health Alliance for Records Exchange.

(h) **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 the State Health Alliance for Records Exchange.

(i) **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 the State Health Alliance for Records Exchange.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

25 CAR § 20-106. Access to and use of disclosure information.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology and all participating entities.

(b) **Compliance with law.**

(1) All disclosures of protected health information through the State Health Alliance for Records Exchange and the use of information obtained through the State Health Alliance for Records Exchange shall be consistent with all applicable federal, state, and local laws and rules and shall not be used for any unlawful discriminatory purpose.

(2) 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.

(c) **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.

(d) **Purposes.**

(1) A participating entity may request health information through the State Health Alliance for Records Exchange only for purposes permitted by applicable law.

(2)(A) Each participating entity shall provide or request health information through the State Health Alliance for Records Exchange only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and rules and these policies.

(B) Information may not be requested for marketing-related purposes without specific patient authorization.

(C) Under no circumstances may information be requested for a discriminatory purpose.

(3) In the absence of a permissible purpose, a participating entity may not request information through the State Health Alliance for Records Exchange.

(e) **Office policies.** Uses and disclosures of and requests for protected health information via the State Health Alliance for Records Exchange shall comply with all office policies, including, but not limited to, the office policy on minimum necessary, 25 CAR § 20-108, and the office policy on information subject to special protection, 25 CAR § 20-107.

(f) **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.

(g) **Accounting of disclosures.**

(1) Each participating entity disclosing protected health information through

the State Health Alliance for Records Exchange 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.

(2) 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.

(3) 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.

(h) **Audit logs.** Participating entities and the office shall develop an audit log capability to document which participating entities posted and accessed the information about an individual through the State Health Alliance for Records Exchange and when such information was posted and accessed.

(i) **Authentication.**

(1) The office shall follow a uniform authentication process for verifying and authenticating the identity and authority of each authorized user and participating entity.

(2) Individuals whose identities and authority have been authenticated by this process are referred to in these policies as "authorized users".

(3) Participating entities shall be entitled to rely on the State Health Alliance for Records Exchange'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.

(4) This process is described in greater detail in the OHIT Security Policies and Security Framework.

(j) **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 BA agreements.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-107(b)(2) as follows: "See 45 C.F.R. § 164.5300)".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-107(d)(2)(A) as follows: "45 C.F.R. § 164.502(a),(b)".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-107(e) as follows: "45 C.F.R. § 164.502(b)".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-107(g)(1) as follows: "See 45 C.F.R. § 164.528. For HIPAA Covered Entities, this is currently required by law".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-107(h) as follows: "See 45 C.F.R. § 164.316, 164.308(a)(1)(i)".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-107(i)(1) as follows: "45 C.F.R. §§ 164.514(h), 164.312(d)".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-107(i)(1) as follows: "See Connecting for Health, "Authentication of System Users."

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L.

No. 104-191.

"BA" means business associate.

25 CAR § 20-107. Information subject to special protection.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology and all participating entities.

(b) **Special protection.**

(1) The operation of the State Health Alliance for Records Exchange and these policies are intended to comply with the HIPAA privacy standards.

(2) Some health information may be subject to special protection under federal, state, and/or local laws and rules.

(3) Each participating entity shall determine and identify what information is subject to special protection under applicable law prior to disclosing any information through the State Health Alliance for Records Exchange.

(4) Each participating entity is responsible for complying with such laws and rules.

(5) Participating entities should not make protected health information requiring special protection available to the State Health Alliance for Records Exchange.

(c) **Information not furnished.**

(1) For the State Health Alliance for Records Exchange 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)(A) Accordingly, participating entities accessing and using another participating entity’s information obtained through the State Health Alliance for Records Exchange should assume that the information made available does not include any of the following:

(i)*(a)* Alcohol and substance abuse treatment program records;

(b) See 42 C.F.R. Part 2.

(ii)*(a)* Records of predictive genetic testing performed for genetic counseling purposes.

(b) See The Genetic Information Nondiscrimination Act of 2008 (Pub. L. 110-233, 122 Stat. 881, enacted May 21, 2008); and

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

(B) This list is suggestive only.

(C) Other records may be added to the list.

(5) Participating entities should assume the above listed records are not included in the State Health Alliance for Records Exchange.

(d) **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 BA agreements.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

"BA" means business associate.

25 CAR § 20-108. Minimum necessary.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology, all participating entities, and their BAs and contractors.

(b) **Requests.**

(1) Each participating entity shall request only the minimum amount of health information through the State Health Alliance for Records Exchange as is necessary for the intended purpose of the request.

(2) The minimum necessary policy does not apply to requests by health care providers for treatment purposes.

(c) **Uses and disclosures.**

(1) Each participating entity shall use and disclose only the minimum amount of health information obtained through the State Health Alliance for Records Exchange as is necessary for the purpose of each use or disclosure.

(2) Each participating entity shall share health information obtained through the State Health Alliance for Records Exchange and allow access to such information only those workforce members, agents, and contractors who need the information in connection with their job functions or duties.

(3) Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this minimum necessary policy.

(d) **Workforce, BAs, and contractors**. Each participating entity shall adopt and apply policies to limit access to the State Health Alliance for Records Exchange 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.

(e) **Entire medical record.**

(1) 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.

(2) This limit does not apply to disclosures to or requests by a health care provider for treatment purposes or disclosures required by law.

(f) **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.

(g) **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 BA agreements.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

"BA" means business associate.

25 CAR § 20-109. Workforce, agents, and contractors.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology and all participating entities and their BAs and contractors.

(b) **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 the State Health Alliance for Records Exchange, and to train and supervise its authorized users to the extent applicable to their job responsibilities.

(c) **Authorized users.**

(1)(A) All authorized users, whether members of a participating entity's workforce or members 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.

(B) This shall include familiarity with applicable privacy and security policies of the participating entity, BA, or contractor, as applicable.

(2) 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.

(3) The office shall have the authority under the participation agreement to suspend, limit, or revoke access authority to the State Health Alliance for Records Exchange for any authorized user or participating entity for violation of the office's privacy and security policies or any federal or state law.

(d) **Access to system.**

(1) Each participating entity shall allow access to the State Health Alliance for Records Exchange only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the State Health Alliance for Records Exchange and/or release or obtain information through the State Health Alliance for Records Exchange.

(2) No workforce member, agent, or contractor shall be provided with access to the State Health Alliance for Records Exchange without first having been trained on these policies, as set forth below.

(e) **Training.**

(1) Each participating entity shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the State Health Alliance for Records Exchange to ensure compliance with these policies.

(2) 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.

(f) **Discipline for noncompliance.**

(1) 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.

(2) Such discipline measures shall include, but not be limited to, verbal and written warnings, demotion, and termination and provide for retraining where appropriate.

(g) **Reporting of noncompliance.**

(1) Each participating entity shall have a mechanism for, and shall encourage, all workforce members, agents, and contractors to report any noncompliance with these policies to the participating entity.

(2) Each participating entity also shall establish a process for individuals whose health information is included in the State Health Alliance for Records Exchange to report any noncompliance with these policies or concerns about improper disclosures of

information about them.

(h) **Enforcing BA agreements and contractor agreements.** Each participating entity shall require in any relationship with a BA, 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:

(1) Such third party and any member of its workforce shall be subject to these policies when accessing, using, or disclosing information through the system;

(2) 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

(3) 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.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. This section, as promulgated prior to the codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-110(e)(1) as follows: "See 45 C. F. R. § 164.530(b)".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-110(f)(1) as follows: "45 C. F. R. § 164.530 (e)".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-110(g)(1) as follows: "45 C.F.R. § 164.530(a),(d)".

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

"BA" means business associate.

25 CAR § 20-110. Amendment of data.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology and all participating entities.

(b) **Accepting amendments.**

(1) Each participating entity shall comply with applicable federal, state, and local laws and rules regarding the amendment of health information.

(2)(A) If an individual or treating physician requests, and the participating entity accepts, an amendment to the health information, the participating entity, assisted by the office shall make reasonable efforts to inform other participating entities that accessed or received such information through the State Health Alliance for Records Exchange 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.

(B) Only the participating entity responsible for the record being amended may accept an amendment.

(C) If one participating entity believes there is an error in the record of another participating entity, it shall contact the responsible participating entity.

(c) **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 BA agreements.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-111(b)(1) as follows: "45 C.F.R. § 164.526".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-111(b)(1) as follows: "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".

"BA" means business associate.

25 CAR § 20-111. Requests for restrictions.

(a) **Scope and applicability.** This policy applies to all participating entities.

(b) **Recipient responsibility.** A participating entity, when accessing the State Health Alliance for Records Exchange 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.

(c) **Data provider responsibility.**

(1)(A) If a participating entity agrees to an individual's request for restrictions, as permitted under the HIPAA privacy rule, such participating entity shall ensure that it complies with the restrictions when releasing information through the State Health Alliance for Records Exchange.

(B) This shall include not exchanging the individual's protected health information through the State Health Alliance for Records Exchange and opting the individual out of the State Health Alliance for Records Exchange, if required by the restriction.

(C) Participating entities should advise individuals that opting out only affects access, use, and disclosure of their protected health information through the State Health Alliance for Records Exchange.

(2) 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.

(3) 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 the State Health Alliance for Records Exchange.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR §§ 20-112(c)(1)(A) and (c)(3) as follows: "45 C.F.R.§164.522".

This section, as promulgated prior to codification in the Code of Arkansas Rules contained a footnote to 25 CAR § 20-112(c)(3) as follows: "Under the HIPAA privacy rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 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."

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

25 CAR § 20-112. Mitigation.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology, all participating entities, and their BAs and contractors.

(b) **Duty to mitigate.**

(1) Each participating entity shall implement a process to mitigate, and shall mitigate and take appropriate remedial action against, any harmful effect that is known to the participating entity of a use or disclosure of protected health information through the State Health Alliance for Records Exchange that is in violation of applicable laws and/or rules and/or these policies by the participating entity or its workforce members, agents, and contractors.

(2) 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.

(c) **Duty to cooperate.**

(1) 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 the office and with another participating entity that has the primary obligation to mitigate a breach.

(2) 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.

(d) **Notification to the office.**

(1) A participating entity primarily responsible to mitigate shall notify the office Privacy Officer of all events requiring mitigation and of all actions taken to mitigate.

(2) The office may facilitate the mitigation process if asked.

(3) The office shall provide training on breach mitigation.

(e) **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 BA agreements.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. "BA" means business associate.

25 CAR § 20-113. Investigations— Incident response system.

(a) **Scope and applicability.** This policy applies to the Office of Health Information Technology, all participating entities, and their BAs and contractors.

(b) **Individual complaints.**

(1) Any individual may submit a complaint about a use or disclosure of

protected health information by the Office of Health Information Technology to either the Office of Health Information Technology or the United States Secretary of Health and Human Services in Washington, D.C.

(2) If the individual wants to file a formal complaint with the Office of Health Information Technology, he or she should be directed to the Office of Health Information Technology Privacy Officer.

(3) If the individual wants to file his or her complaint with the United States Secretary of Health and Human Services, he or she should be directed to the United States Office for Civil Rights website (www.hhs.gov/ocr/hipaa).

(4) The Office of Health Information Technology Privacy Officer will document each privacy complaint received including in the documentation a brief description of and/or the basis for the complaint.

(5) The Privacy Officer will supplement the initial documentation to include documentation of the investigation and any actions taken in response to the complaint.

(6) All documentation relating to the individual's complaint will be maintained for a minimum of six (6) years.

(c) **Duty to investigate.**

(1) Each participating entity shall promptly investigate reported or suspected privacy breaches implicating privacy or security safeguards deployed by the Office of Health Information Technology, or its contractors, according to its own policies.

(2) Upon learning of a reported or suspected breach, the participating entity shall notify the Office of Health Information Technology within five (5) 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.

(3) The Office of Health Information Technology shall participate in the investigation and remedial actions taken.

(4) The Office of Health Information Technology need not be notified of specific workforce disciplinary actions.

(5) Each investigation shall be documented.

(6) At the conclusion of an investigation, a participating entity shall document its findings and any action taken in response to an investigation.

(7) A summary of the findings shall be sent to the Office of Health Information Technology.

(d) **Compliance with HIPAA security rule.**

(1) The Office of Health Information Technology will comply with the HIPAA security rule.

(2) 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.

(e) **Training and enforcement.**

(1) Each participating entity that may have access to patient data via the State Health Alliance for Records Exchange must appropriately train its personnel and inform them that any breach of confidentiality is actionable.

(2) Each participating entity should follow and enforce its own confidentiality policies and disciplinary procedures.

(f) **Notification of breach.**

(1) As a BA, the Office of Health Information Technology must report any breaches and/or security incidents to the particular data provider whose data was improperly used.

(2) Each participating entity must agree to inform the Office of Health Information Technology of any breach of confidentiality.

(g) **Incident response.**

(1) The Office of Health Information Technology shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by a participating entity or discovered by the Office of Health Information Technology.

(2) The incident response system shall include the following features, each applicable as determined by the circumstances:

(A) Cooperation in any investigation conducted by the participating entity or direct investigation by the Office of Health Information Technology;

(B) 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;

(C) Cooperation in any mitigation steps initiated by the participating entity;

(D) Furnishing audit logs and other information helpful in the investigation;

(E) Developing and disseminating remediation plans to strengthen safeguards or hold participating entities or authorized users accountable;

(F) Any other steps mutually agreed to as appropriate under the circumstances; and

(G) Any other step required under the incident reporting and investigation system contained in the Office of Health Information Technology security policies.

(g) **Office cooperation.** The Office of Health Information Technology 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 the Office of Health Information Technology conduct or the conduct of another participating entity or authorized user, or the adequacy or integrity of system safeguards.

(h) **Participating entity cooperation.** Each participating entity shall cooperate with the Office of Health Information Technology in any investigation of the Office of Health Information Technology or of another participating entity into the Office of Health Information Technology'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 the Office of Health Information Technology or the other participating entity, when the investigation implicates such participating entity's compliance with the Office of Health Information Technology policies or the adequacy or integrity of system safeguards.

(i) **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 BA agreements.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

"BA" means business associate.

25 CAR § 20-114. Authorized user controls.

(a) **Scope and applicability.**

(1) This policy applies to the Office of Health Information Technology, all participating entities, and their BAs and contractors.

(2) This policy is to be read and applied in conjunction with the office security policy.

(b) **Participating entity responsibilities.** Each participating entity is responsible to:

(1)(A) 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.

(B) For participating entities that have their own system administrator, this shall ordinarily be the State Health Alliance for Records Exchange administrator;

(2) Designate its own authorized users from among its workforce and designate BAs and contractors authorized to act as authorized users on its behalf;

(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 the office's privacy policies and with the terms of the participating entity's privacy policies and the BA agreement as applicable.

(4)(A) 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.

(B) 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.

(C) For participating entities without their own system administrator, immediately notify the office security officer of the change so that the office may revoke access authority.

(D) 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; and

(5) Hold their authorized users accountable for compliance with the office and the participating entity's policies and, as applicable, the terms of any BA agreement.

(c) **Office responsibilities.** The office or the office's designee is responsible to:

(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) Train and supervise its own authorized users on these policies and the standard terms required by its BA agreement with participating entities;

(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 the office as required by these policies or the terms of its BA agreement in the event of breach or noncompliance;

(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; and

(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, office policies, or the terms of the user agreement, if the office determines that doing so is necessary for the privacy of individuals or the

security of the State Health Alliance for Records Exchange.

(d) **Office security procedures.** The details of how to grant and revoke access authority are contained in the office security framework.

(e) **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 BA agreements.

Authority. Arkansas Code §§ 25-42-105 [repealed], 25-43-811.

Codification Notes. "BA" means business associate.