

One Health Record®

AHIE Policies and Procedures



THESE POLICIES AND PROCEDURES ARE REQUIRED FOR PARTICIPATION IN ALABAMA'S HEALTH INFORMATION EXCHANGE:

One Health Record®

THESE POLICIES AND PROCEDURES DO NOT SUPPLANT OR PREEMPT ANY FEDERAL AND STATE LAWS APPLICABLE TO HEALTH CARE PROVIDERS OR OTHER ENTITIES. FOLLOWING THESE POLICIES AND PROCEDURES DOES NOT PROTECT A PARTICIPANT OR ANOTHER ENTITY FROM LIABILITY UNDER APPLICABLE LAW.

One Health Record® IS INTENDED TO BE USED AS AN INFORMATION GATHERING TOOL TO AID HEALTH CARE PROVIDERS AND OTHER PARTICIPANTS. THE USE OF One Health Record® DOES NOT ELIMINATE A PROVIDER'S NEED TO EXERCISE PROFESSIONAL JUDGMENT IN CLINICAL DECISION MAKING. One Health Record® DOES NOT WARRANT OR GUARANTEE THE ACCURACY OR COMPLETENESS OF THE INFORMATION MADE AVAILABLE FROM PARTICIPANTS THROUGH AHIE.

Most Recent Update April 17, 2014

Approved by HIE Commission

Table of Contents

I.	<u>BACKGROUND & PURPOSE</u>	4
II.	DEFINITIONS	4
1.	AHIE GOVERNING AUTHORITY.	13
2.	OBLIGATIONS OF AHIE AND PARTICIPANT.	13
	a. AHIE’s Obligations	13
	b. Participant’s Obligations	14
3.	PARTICIPATION IN ONE HEALTH RECORD® WITHOUT INDIVIDUAL AUTHORIZATION.	15
4.	OPT-OUT PROCEDURES.	15
	a. Opt-out Option under One Health Record®.	15
	b. Revocation of Opt-Out Option.	16
	c. Participant’s Maintenance of Opt-Out Documentation	16
	d. Participant’s Withholding Care Based on Opt-Out Status.	16
5.	REQUESTS, USES AND DISCLOSURE OF INFORMATION.	16
	a. Use and Disclosures must comply with all laws and not be made for Unlawful or Discriminatory Purposes.	16
	b. Requests and Disclosures may be made for only Permitted Purposes.	17
	c. Uses and Disclosures must comply with all AHIE Policies.	17
	d. Uses and Disclosures must comply with Participant’s internal Polices.	17
	e. Participant shall document disclosures to comply with HIPAA.	17
	f. Participant shall maintain an access Audit Log.	17
6.	INFORMATION SUBJECT TO SPECIAL PROTECTION.	18
7.	MINIMUM NECESSARY INFORMATION.	18

8.	ACCESS TO AHIE.....	18
a.	AHIE Access is limited to those with legitimate and appropriate need.....	18
b.	AHIE Access must be monitored by Participant.	18
c.	Security for AHIE Access must be maintained by Participant.	18
d.	Participant must train for AHIE Access.....	19
9.	PREVENTION OF AND SECURITY BREACHES.....	19
a.	Participant must implement mitigation procedures for breaches.....	19
b.	Participant must identify, respond, and document breaches.	19
c.	Participant must report actual or suspected breaches.	19
d.	Participant is subject to audits of internal security practices.....	20
10.	QUALITY OF INFORMATION.....	20
11.	RIGHT TO REQUEST AMENDMENT OF HEALTH INFORMATION.....	20
12.	ENFORCEMENT.....	20

I. Background & Purpose

The Alabama Health Information Advisory Commission is a collaborative formed in 2010 to create, champion, and sustain a secure, Alabama health information exchange (AHIE) that will dramatically improve the safety, efficiency, and quality of health care in Alabama. Currently, it is a voluntary effort chaired by the Alabama Medicaid Agency (as the State Designated Entity) representing a collaborative approach to meeting the challenge of health information technology adoption and interoperability for the entire state of Alabama. The Commission is committed to improving healthcare IT interoperability throughout the state through the implementation of an Alabama HIE. To that end, this policy framework defines the policies for community clinical data exchange via the One Health Record® system. The policies establish baseline operating rules for AHIE, as the provider of AHIE services, and for AHIE Participants, as users of the AHIE.

The following policies provide basic, minimum policy requirements for Participants who have executed an Alabama Health Information Exchange DURSA/Participation Agreement and Business Associate Agreement who will be engaged in exchanging electronic health information through AHIE.

A Participant's failure to comply with the Policies and Procedures stated below constitutes a breach of the AHIE Participation Agreement and may result in termination of the Agreement, denial of access to the AHIE network, or financial penalties as discussed in the AHIE Participation Agreement and herein.

These Policies and Procedures may be revised and updated periodically in accordance with the Participation agreement and this AHIE Policy Manual in response to changes in applicable laws and regulations, changes in technology and standards, or other factors affecting the governance and operation of AHIE. The current version of the AHIE policies will be available on the AHIE website. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Policies and Procedures.

Compliance with and adherence to these Policies and Procedures will be monitored and enforced by the AHIE staff under the guidance of the Governing Authority. Any suggested additions or changes to these policies should be submitted to the Governing Authority for consideration.

II. Definitions

Terms used in the AHIE Policies and Procedures that are specifically defined in the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") enacted as part of the American Recovery and Reinvestment Act of 2009, and its attendant regulations and guidance, shall have the same meaning as set forth in HIPAA. A change to HIPAA which modifies any defined HIPAA term, or which alters the regulatory citation for the definition shall be deemed incorporated into this Agreement.

- 1.1 **"Adapter" means the 'system' that holds a data provider's patient demographic and clinical data, identifies that data to a statewide Record Locator Service (Enterprise Master Patient Index) and allows for a "real time" sharing of clinical information (based on role based access controls) from disparate electronic data contained on other linked Adapters.**
- 1.2 **"Administrative safeguards" means administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and PII and to manage the conduct of the entity's workforce in relation to the protection of that information. Administrative safeguards include policies and procedures, workforce training, risk management plans, and contingency plans.**
- 1.3 **"AHIE" means the Alabama Health Information Exchange (also known as One Health Record®); the AHIE provides the core system components such as the RLS, as well as functions as a Data provider on behalf of other electronic data sources.**
- 1.4 **"AHIE Performance and Service Specifications" shall refer to the AHIE Test Approach and the AHIE Interface Specifications contained in the AHIE Policy Manual and as amended from time to time.**
- 1.5 **"AHIE Policy Manual" means the documents approved by the Governing Authority containing these definitions, the AHIE Performance and Service Specifications, the AHIE Policies and Procedures, the Participation Agreement, the Business Associate Agreement, and any other documents included by the Governing Authority of One Health Record®. Each Participant is contractually bound to the contents of the AHIE Policy Manual, as it may be amended. The Governing Authority shall review and may amend the AHIE Policy Manual from time to time as provided in the Participation Agreement.**
- 1.6 **"AHIE Policies and Procedures" shall mean the policies and procedures adopted by the Governing Authority that describe management, operation, and participation in AHIE contained in the AHIE Policy Manual, as it may be amended from time to time.**
- 1.7 **"Audit" shall mean a review and examination of records (including logs), and/or activities to ensure compliance with the Participation Agreement and the AHIE Policy Manual and to ensure accuracy of the data transmission and conversion of data by the Adapter. This review can be manual, automated or a combination of both.**
- 1.8 **"Audit Host" shall mean any designee the AHIE contracts with to provide the audit services to support the AHIE and the System.**
- 1.9 **"Authorization" shall meet the requirements and have the meaning set forth at 45 CFR § 164.508(b) of the HIPAA Regulations.**

- 1.10 "Authorized User" means an individual Participant or an individual Participant User designated to use the Services on behalf of the Participant. Authorized Users would receive their rights to use the Services either by registering as Participants themselves or through another organization that registers as a Participant and designates individuals who will be authorized to use the Services on the Participant's behalf. For example, an Authorized User may be an individual physician who registers as a Participant. In addition, an Authorized User may be a member of that physician's office staff designated by the physician, or any one of a number of a hospital's employees and/or medical staff members authorized by the hospital to act as Authorized Users under the hospital's registration as a Participant.**
- 1.11 "Business Associate" means a non-Workforce Member, who, on behalf of a covered entity or an organized health care arrangement, performs or assists in the performance of one of the following:**
- A function or activity involving the use or disclosure of PHI and PII, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and re-pricing.**
 - Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services for such covered entity or organized health care arrangement.**
- 1.12 "Business Associate Agreement" or "BAA" means a contract between a covered entity and a business associate that does all of the following:**
- Establishes the permitted and required uses and disclosures of PHI by the business associate.**
 - Provides that the business associate will use PHI only as permitted by the contract or as required by law, use appropriate safeguards, report any disclosures not permitted by the contract, ensure that agents to whom it provides PHI will abide by the same restrictions and conditions, make PHI available to individuals and make its record available to U.S. Department of Health and Human Services.**
 - Authorizes termination of the contract by the Department if the Department determines that there has been a violation of the contract.**
- 1.13 "Collect/Collection" means the acquisition or receipt of information, including PHI and PII.**
- 1.14 "Core Services" shall include the following services provided by AHIE: Master Patient Index (MPI), Record Locator Service (RLS), Terminology Standards and Services, Public Key Infrastructure (PKI) certificate-based encryption and**

authentication, Audit/Log of Participant document transport, DHEC Immunization Registry exchange, RX (prescription) Hub and NHIN Connect Gateway.

- 1.15 "Consent" shall be understood in the context of 45 C.F.R. § 164.506 and §164.508 of the HIPAA Regulations.
- 1.16 "Corrective Measures" means actions taken to address a security breach or privacy violation, with the intent to counteract the breach or violation and reduce future risks.
- 1.17 "Covered Entity" means the Administrative Simplification standards adopted by Health and Human Services (HHS) under HIPAA that apply to any entity that is a health care provider that conducts certain transactions in electronic form, a health care clearinghouse, or a health plan.
- 1.18 "Data" shall mean that information which is requested or sent by a Participant to another Participant through AHIE. This includes, but is not limited to, PHI, de-identified data, pseudonymized data and metadata.
- 1.19 "Data Aggregation" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR § 164.501.
- 1.20 "De-identified" means that all identifying information related to an individual as set forth in the HIPAA Privacy and Security Rule (45 CFR Section 164.514 (b)), are removed from PHI.
- 1.21 "Designated Record Set" shall have the meaning given to the term under the Privacy Rule, including, but not limited to, 45 CFR §164.501.
- 1.22 "Disclose/Disclosure" means the release, transfer, exchange, provision of access to, or divulging in any other manner of information outside the person or entity holding the information.
- 1.23 "DURSA" means the Data Use and Reciprocal Support Agreement, which is a single agreement that establishes the rules of engagement and obligations to which all Participants agree and that all Participants sign as a condition of joining One Health Record® (also known as the Participation Agreement).
- 1.24 "Effective Date" shall mean the date on which a Participant executes the DURSA/Participation Agreement.
- 1.25 "Electronic Protected Health Information" and/or "EPHI" shall have the same meaning as the term "electronic protected health information" in 45 CFR § 160.103, and shall include, without limitation, any EPHI provided by Covered Entity or created or received by Business Associate on behalf of Covered Entity.

- 1.26 "Electronic Health Record" or "EHR" shall have the meaning given to that term under Section 13400(5) of HITECH.
- 1.27 "Executive Director" means the Executive Director of the AHIE.
- 1.28 "Governing Authority" shall mean the entity which is responsible for administering One Health Record® and fulfilling the roles and responsibilities described herein or any governing authority given such governance authority over the AHIE pursuant to legislation.
- 1.29 "Health Care Operations" shall mean activities of a Participant providing treatment to an individual relating to quality assessment and improvement, evaluations related to the competence of treating providers or necessary administrative and management activities all as defined in the HIPAA Privacy Regulations, 45 CFR Section 164.501.
- 1.30 "Health Information" shall mean any information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
- 1.31 "Health Care Organization" or "HCO" means health care providers, public health agencies, payors, and entities offering patient engagement services, such as Patient Health Records.
- 1.32 "Health Information Exchange" or "HIE" shall mean the electronic movement of health-related information according to nationally recognized standards.
- 1.33 "Health Information Organization" or "HIO" means an organization that oversees and governs the exchange of health-related information locally or regionally among health care organizations according to nationally recognized standards.
- 1.34 "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, as amended, and related regulations (45 CFR. Parts 160-164).
- 1.35 "HITECH" means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII and Title IV of the American Recovery and Reinvestment Act of 2009, Public Law 111-5. specifically Subtitle D, that outlines the obligations of HIEs with respect to HIPAA.
- 1.36 "Individual" means the person who is the subject of the PHI, but also includes a person who qualifies as an authorized representative of the patient in accordance with legal requirements, whose PHI may be transmitted by Participants via One Health Record®.

- 1.37 **"Individually Identifiable Health Information"** means information that that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer or health care clearinghouse and relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of health care to an individual and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Individually Identifiable Health Information shall have the same meaning as the term is defined in 45 C.F.R. § 160.103.
- 1.38 **"Monitor"** shall mean a review and examination of records (including logs), and/or activities to evaluate the utilization levels, efficiency and technical capabilities of AHIE. This review can be manual, automated or a combination of both.
- 1.39 **"Nationwide Health Information Network or NHIN"** shall mean a secure, nationwide, interoperable health information infrastructure that allows for the exchange of Data between and among Participants in support of the provision of health and healthcare services.
- 1.40 **"Notice"** or **"Notify"** shall mean a notice in writing sent to the appropriate Participant's representative at the address listed in this Agreement or to the Governing Authority.
- 1.41 **"ONC"** shall mean the Office of the National Coordinator for Health Information Technology in the Office of the Secretary, U.S. Department of Health and Human Services.
- 1.42 **"One Health Record®"** means Alabama's Health Information Exchange (also referenced as AHIE)
- 1.43 **"Optional Services"** shall include the following services that AHIE may provide Participants who choose to contract and pay for such services in addition to the Core Services covered under the terms of the Participation Agreement: Clinical Viewer, EMR- Lite, E-prescribe, and Care Coordination Tools.
- 1.44 **"Opt-Out"** refers to an individual's choice to not participate in the sharing of his or her electronic records via One Health Record® and must be given in writing to a Participant
- 1.45 **"ORS"** shall mean the Office of Research and Statistics at the State Budget and Control Board.
- 1.46 **"Participation Agreement"** shall mean the Data Use and Reciprocal Support Agreement, which is a single agreement that establishes the rules of engagement and

obligations to which all Participants agree and that all Participants sign as a condition of joining the AHIE (also known as the DURSA).

- 1.47 "Participant" shall mean any eligible individual, entity, or Health Care Operations worker that is a signatory to the DURSA or Participation Agreement, except for the Governing Authority, with One Health Record® and is registered and authorized to access the HIE.

If the entity or Health Care Operations department within which the individual practices signs a Participant Agreement, the individual is not required to sign a separate Participation Agreement, but must sign a Participant User Agreement. Eligible individuals are health care providers licensed in Alabama and providing health care services within their statutory scope of practice, including medical doctors, dentists, chiropractors, optometrists, podiatrists, pharmacists, physician assistants, and nurse practitioners. Eligible entities are health information organizations and entities within which eligible individuals practice, hospitals, ambulatory surgical facilities, home health agencies, case management providers, telemonitoring providers, pharmacies, and governmental agencies involved in healthcare.

- 1.48 "Payment" shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.
- 1.49 "Permitted Purposes" shall mean the following reasons for which Participant Users may legitimately exchange Data through AHIE:
- Treatment of an Individual with whom the Participant User has a Treatment Relationship;
 - HIPAA permitted uses and disclosures under 45 C.F.R. § 164.512(a) - (d), (h), and (j) - (l), related to (i) an Individual with whom a Participant User has an established Treatment Relationship, or (ii) a public health initiative;
 - A Participant's submission of information required by law, including but not limited to immunization data, quality reporting data, and communicable disease data to a state or federal agency; and
 - Uses and disclosures premised on an Authorization provided by the Individual who is the subject of the Message.
- 1.50 "Personal Health Record" shall mean an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards, including but not limited to those that have been recognized by HHS, and that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for individual.
- 1.51 "Personal Identifiable Information" and/or "PII" means information that identifies the individual whether or not it is specifically health-related or not, or with respect to which there is a reasonable basis to believe the information can be used to

- identify the individual, such as, but not limited to, name, address, phone number, drivers license number, social security number, PHI, banking information, or claims information.
- 1.52 “Persons and Entities” means health care professionals, partnerships, proprietorships, corporations and other types of organizations and their agents when acting on their behalf.
- 1.53 “Physical safeguards” means physical measures, policies and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. Physical safeguards include workstation security and use procedures, facility security plans, data backup and storage, and portable device and media controls.
- 1.54 “Privacy” means an individual’s interest in protecting his or her PHI and the corresponding obligation of those persons and entities, that participate in the AHIE for the purposes of electronic exchange of such information, to respect those interests through fair information practices.
- 1.55 "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information, and Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule"), that are codified at 45 C.F.R. Parts 160 and 164, Subparts A, C, and E and any other applicable provision of HIPAA, and any amendments thereto, including HITECH.
- 1.56 "Protected Health Information" and/or "PHI" means any information that identifies an individual and relates to either the individual’s past, present or future physical or mental health, or the provision of health care to the individual, or the past, present or future payment for health care and shall have the meaning given to the term under the Privacy Rule, including but not limited to, 45 C.F.R. § 160.103, and shall include, without limitation, any PHI provided by or received by a Participant User. Unless otherwise stated in this Agreement, any provision, restriction, or obligation in this Agreement related to the use of PHI shall apply equally to EPHI.
- 1.57 “Recipient” means a Participant who receives PHI and PII through the AHIE.
- 1.58 "Record Locator Service" or “RLS” means the system that identifies and links patients with their data across the linked continuum of care.
- 1.59 "Regional Health Information Organization” or “RHIO" means a health information organization that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community.

- 1.60** "Required By Law" shall have the meaning given to the term under the Privacy Rule including, but not limited to, 45 C.F.R. § 164.103, and any additional requirements created under HITECH.
- 1.61** "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his designee.
- 1.62** "Security" means the physical, technological, and administrative safeguards used to protect PHI and PII.
- 1.63** "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as provided in 45 C.F.R. § 164.304.
- 1.64** "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information in 45 C.F.R. Parts 160 and 164.
- 1.65** "System" means the AHIE's internet-based, authenticated, peer-to-peer computer system and search engine for patient health, demographic, and related information that assists Participant Users in locating Data and facilitates the Adapter of Data held by multiple health care organizations with disparate health information computer applications, and which allows Participant Users to authenticate and communicate securely over an entrusted network to provide access to and to maintain the integrity of Data.
- 1.66** "Transparent" means making information readily and publicly available.
- 1.67** "Technical safeguards" means the technology and the policies and procedures for its use that protect electronic PHI and PII and control access to it.
- 1.68** "Treatment" means the provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between healthcare providers related to a patient; or the referral of a patient for health care from one health care provider or another, or shall otherwise have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.
- 1.69** "Treatment Relationship" means a treatment relationship already in existence between a Participant User and an Individual or an emergency treatment relationship formed due an Individual's emergent condition and requiring immediate treatment by a Participant User.
- 1.70** "Unsecured PHI" shall have the same definition that the Secretary gives the term in guidance issued pursuant to § 13402 of HITECH.

- 1.71 “Use” means the employment, application, utilization, examination, analysis, or maintenance of PHI and PII.
- 1.72 “Workforce Member” means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity is under the direct control of such entity, whether or not paid by the entity; persons who do not fall in these categories, but nonetheless perform services on behalf of the Covered Entity would be considered a Business Associate.

1. **AHIE Governing Authority.**

The Governing Authority of the AHIE shall have the following duties:

- a. to provide policy direction and operational guidance for the AHIE Executive Director who shall serve at the pleasure of the Governing Authority;
- b. to oversee the development, implementation, and operation of AHIE in compliance with all applicable State and federal requirements;
- c. to establish a legal and policy framework for operation and the financial stability of AHIE, consistent with state and federal requirements;
- d. to develop, implement, review and revise the Strategic and Operational Plans for the AHIE as approved by the National Coordinator for Health Information Technology;
- e. to develop and implement Policies and Procedures governing AHIE that are consistent with state and federal law, and include the right of patients to opt out of having their PHI exchanged through AHIE;
- f. to develop the necessary agreements to facilitate the secure exchange of health information through AHIE and among all trading partners; and
- g. to encourage all applicable state agencies to participate in the AHIE.

2. **Obligations of AHIE and Participant.**

a. **AHIE’s Obligations.**

1. One Health Record® shall comply with all applicable federal, state, and local laws and regulations, including but not limited to HIPAA and HITECH, as they pertain to PHI exchanged electronically through the AHIE.
2. One Health Record® shall make rules to ensure that Individuals are provided with a simple and timely means to access and obtain their PHI in a readable form and format.
3. One Health Record® shall make rules to ensure Individuals are provided with a timely means to dispute the accuracy of their PHI and to have erroneous information corrected (but not deleted) or to have a dispute documented if requests to correct are denied.

4. **One Health Record® shall make rules to ensure Individuals have the ability to request and review documentation to determine who accessed their information or to whom it has been disclosed.**
5. **One Health Record® should make publicly available a notice of privacy and/or data practices describing why PHI is collected, how it is used, and to whom and for what reasons it is disclosed.**

b. Participant's Obligations.

1. **Participants shall comply with all applicable federal, state, and local laws and regulations, including but not limited to HIPAA and HITECH, as they pertain to PHI exchanged electronically through the AHIE.**
2. **Each Participant is responsible for remaining current with all applicable laws and regulations and must ensure that it has the requisite, appropriate, and necessary internal policies in place for compliance with applicable laws and regulations.**
3. **Each Participant shall execute and comply with the DURSA (also known as a Participation Agreement) with AHIE, which establishes the mutual responsibilities of One Health Record® and the Participant, prior to beginning electronic exchange of data through One Health Record®.**
4. **Each Participant shall, at all times, comply with all applicable One Health Record® Policies and Procedures. These policies may be revised and updated from time to time upon reasonable notice to the Participant. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these One Health Record® Policies.**
5. **In the event of a conflict between these One Health Record® Policies and Procedures and the Participant's own policies and procedures, the Participant shall comply with the policy that is more protective of individual privacy and security.**
6. **Participants shall be aware of the provisions of certain state laws which are (or may be) more stringent than, and not preempted by HIPAA, such as but not limited to sensitive data like psychotherapy records.**
7. **Each Participant is responsible for using written documentation of their internal policies and these AHIE Policies to facilitate the training of Workforce Members who will handle PHI and PII.**
8. **Each Participant shall develop, maintain, and distribute a notice of privacy and/or data practices that complies with HIPAA, HITECH, and any other applicable law or regulation. Individuals must be advised, in this notice or elsewhere, why PHI is collected, how it is used, to whom and for what reasons it is disclosed, and where public information on this topic can be obtained.**

9. Each Participant must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as those that limit incidental uses or disclosures. [45 CFR 164.530(c)].
10. Participant must provide Individuals with a simple and timely means to access and obtain their PHI in a readable form and format.
11. Participant must provide Individuals with a timely means to dispute the accuracy of their PHI with the Participant's records and to have erroneous information corrected (but not deleted) and to have a dispute documented if requests to correct are denied.
12. Participant must provide Individuals with the ability to request and review documentation to determine who accessed their information or to whom it has been disclosed.
13. Participants are encouraged to be open and transparent with Individuals about the Participant's privacy and security practices and to specifically discuss One Health Record® with Individuals.

3. Participation in One Health Record® without Individual Authorization.

Participant's Notice of Privacy Practices identified in Section 2(b)(8) shall advise Individual's that a Participant may request, use, and disclose protected health information, without an individual's authorization, for Permitted Purposes, such as treatment, payment, or health care operations purposes.

The transfer of information through One Health Record® is a method of disclosing PHI electronically for Permitted Purposes, like treatment, payment, or health operations purposes. Unless an Individual chooses to Opt-Out of participation in One Health Record® as provided in Section 4(a), a Participant's electronic disclosure of PHI through One Health Record® for treatment, payment, and health care operations for an Individual, without an Individual's authorization, is permitted. [See 45 C.F.R. § 164.502(a)(1); 45 C.F.R. § 164.506(c).]

4. Opt-Out Procedures.

a. Opt-out Option under One Health Record® .

While disclosures of PHI through One Health Record® for treatment, payment, or health care operations, without an Individual's authorization, is permitted, One Health Record® allows an Individual to choose not to participate in the electronic sharing of his or her protected health information through One Health Record® (also known as the "Opt-Out" option).

Participant must implement processes to allow any Individual to choose to Opt-Out of One Health Record® , meaning having information regarding that Individual included in or

made available or exchanged through AHIE, except for certain health information required to be submitted by federal or state law.

At this time, an Individual's decision to Opt-Out of having information exchanged or made available via AHIE is global. If an Individual chooses to Opt-Out, no information regarding the patient will be exchanged or made available from any Participant unless required by law.

If an Individual chooses not to participate in One Health Record® for the sharing of electronic records, the Individual must provide notice of Opt-Out to a Participant in writing, in a form and manner determined by the Participant.

Once an Individual has opted out of having his or her information included in or made available through AHIE, the Participant shall, within 2 business days, take appropriate steps to ensure the Individual's information shall no longer be available from Participant through AHIE and notify One Health Record® as to an Individual's changed status. Each Participant must develop and implement appropriate mechanisms to ensure no information about an Individual who has opted out shall be included in or made available through AHIE.

b. Revocation of Opt-Out Option.

An Individual who has opted out of having his or her information from Participant available through One Health Record® may choose at a later time to have his or her information from Participant included in the AHIE. The Individual must request in writing, in a form or manner determined by Participant, that the Participant make the Individual's information available through AHIE. If an Individual chooses to revoke his or her Opt-Out (opting-back into to the AHIE), all available information regarding that Individual may be accessed through AHIE.

c. Participant's Maintenance of Opt-Out Documentation

Each Participant shall document and maintain documentation of all written Opt-Out or Revoke Opt-Out decisions from Individuals.

d. Participant's Withholding Care Based on Opt-Out Status

Participants 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 transferred electronically through One Health Record® and shall make every reasonable effort to avoid any adverse impact on the quality of care.

5. Requests, Uses and Disclosure of Information.

- a. Use and Disclosures must comply with all laws and not be made for Unlawful or Discriminatory Purposes.

All disclosures of health information through AHIE and the use of information obtained through AHIE shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful or discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing 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.

b. Requests and Disclosures may be made for only Permitted Purposes.

A Participant, including its Authorized Users, may request health information through AHIE only for Permitted Purposes. Each Participant shall request health information through AHIE only to the extent necessary and only for Permitted Purposes. Information received for a Permitted Purpose must not be disclosed to any third party for a non-Permitted Purpose unless required by applicable state and federal laws. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a Permitted Purpose, a Participant may not request information through AHIE.

c. Uses and Disclosures must comply with all AHIE Policies.

Uses and disclosures of and requests for health information through AHIE shall comply with all AHIE Policies including, but not limited to, the AHIE Policies on Minimum Necessary Information and Information Subject to Special Protection, included herein.

d. Uses and Disclosures must comply with Participant's internal Policies.

Each Participant 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.

e. Participant shall document disclosures to comply with HIPAA.

Each Participant disclosing health information through AHIE shall implement a system to document such information as may be necessary for compliance with the HIPAA Privacy Rule's accounting of disclosures requirement. 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 Participant must be able to provide information required for the disclosing Participant to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement.

f. Participant shall maintain an access Audit Log.

Participant shall maintain an audit log documenting who of Participant's employees and/or contractors posted and accessed the information about an Individual through AHIE and when such information was posted and accessed. Upon request, Participant shall provide patients with an accounting of who has posted and who has accessed information about them through AHIE and when such information was accessed, or alternatively, provide an Individual access to One Health Record®.

6. Information Subject to Special Protection.

Each Participant shall determine and identify what information is subject to special protection (e.g., substance abuse, mental health, and HIV) under applicable laws and regulations prior to disclosing any information through AHIE. Each Participant is responsible for complying with applicable laws and regulations including those that govern and require special protection of information in the portions of Participant's electronic medical record system and the Participant's other systems that interact with AHIE. Participants are responsible for complying with governing laws and regulations and AHIE policies for appropriately designating information that requires special protection under law. If deemed necessary or appropriate, Participants may withhold patient related information from AHIE as long as no statutory or regulatory requirement contravenes this.

7. Minimum Necessary Information.

Consistent with applicable HIPAA exceptions, each Participant shall access only the minimum amount of an Individual's health information through AHIE as is necessary for the intended Permitted Purpose of the request, and each Participant shall use only the minimum amount of health information obtained through AHIE as is necessary for the purpose of such use. Each Participant shall only share health information obtained through AHIE with, and allow access to, such information by those employees, agents, and contractors who need the information in connection with a duly assigned job function or duty and use that information for a Permitted Purpose. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

8. Access to AHIE.

- a. **AHIE Access is limited to those with legitimate and appropriate need.**

Each Participant shall allow access to AHIE only by those Workforce Members, agents, or contractors who have a legitimate and appropriate need to use AHIE for a Permitted Purpose.

- b. **AHIE Access must be monitored by Participant.**

Each Participant shall monitor AHIE access and verify that each Workforce Member, agent, or contractor has completed the training program required by these AHIE Policies and Procedures as set forth below.

- c. **Security for AHIE Access must be maintained by Participant.**

Each Participant's Workforce Members, agents, or contractors shall be assigned a specific and distinct log-on identifier and private passcode required for AHIE access. Participant is responsible for maintaining the security of all log-on identifiers. Participants shall develop, implement, and enforce internal policies governing the use of log-on identifiers and passcodes. At a minimum, each Participant's internal policies must forbid the sharing of

log-on identifiers and passcodes, include a system for conducting internal audits to identify improper access and breaches, and allow for immediate termination of access to AHIE in the event of improper use or breach. No Workforce Member, agent, or contractor shall be provided with access to AHIE or with a log-on identifier or passcode without first having been trained on AHIE Policies and Procedures, as set forth below.

d. Participant must train for AHIE Access.

Each Participant shall develop and implement a training program for its Workforce Members, agents, or contractors who will have access to AHIE, to ensure compliance with federal and state laws and regulations and One Health Record® Policies. [45 CFR 164.530(b)]. The training shall include, but is not limited to, a detailed review of AHIE Policies and Procedures, confidentiality of PHI under HIPAA, HITECH, and other applicable laws, access of AHIE and disclosures for Permitted Purposes, Opt-Outs, security and violations of AHIE. Each Participant must document and maintain documentation of training for all Workforce Members, agents, or contractors given access to AHIE by the Participant. Each trained Workforce Member, agent, or contractor shall sign a representation that he or she received, read, and will adhere to the AHIE Policies and Procedures.

9. Prevention and Security Breaches.

PHI and PII shall be protected by AHIE and Participant with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure in violation of federal and state laws and these One Health Record® Policies. [45 C.F.R. § 164.530(c); 164.308, 164.310, and 164.312].

a. Participant must implement mitigation procedures for breaches.

Each Participant shall implement a process to mitigate, and shall mitigate and take appropriate remedial action to the extent practicable, any harmful effect that is known about improper access or the use or disclosure of health information that is in violation of applicable laws and/or regulations, Participant policies, or One Health Record® Policies. [45 CFR 164.530(f)].

b. Participant must identify, respond to, and document breaches.

Each Participant shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes. [45 CFR 164.308(a)(6)].

c. Participant must report actual or suspected breaches.

Each Participant shall report any violation of an actual or suspected breach of the AHIE Policies and Procedures, regardless of any assessment of harm, to AHIE in accordance with the terms of the Business Associate Agreement. This reporting requirement is in addition to any reporting required by applicable federal and state law.

d. Participant is subject to audits of internal security practices.

At any given time, Participant shall be subject to audits of internal security practices and must verify security practices upon request by AHIE or its designee.

10. Quality of Information.

Each Participant is responsible for maintaining the quality and security of information entered into Participant's Electronic Medical Records (EMR) and made available to other Participants through AHIE. AHIE is not responsible for verifying or correcting any information made available by Participant through AHIE.

11. Right to Request Amendment of Health Information.

Each Participant shall comply with applicable federal, state and local laws and regulations regarding an Individual's right to request amendment of PHI. [45 CFR 164.526].

12. Enforcement.

The Executive Director or his designee must investigate any report or complaint of a breach or inappropriate access, use, or disclosure of patient information exchanged through AHIE or violation of the AHIE Policy Manual and issue a letter of findings, which includes appropriate sanctions as necessary.

In the event that One Health Record® becomes aware of any actual or suspected breach, either through One Health Record's® own detection, notification by a Participant, consumer complaint or otherwise, One Health Record® will comply with the breach notification laws and more specifically:

- 1) Notify any Participants whose data is affected by the breach.
- 2) Investigate (or require the applicable Participant to investigate), without unreasonable delay, the scope and magnitude of such actual or suspected breach, and identify the root cause of the breach.
- 3) Mitigate (or require the applicable Participant to mitigate) to the extent practicable, any harmful effect of such breach that is known to One Health Record® or the Participant. One Health Record's® mitigation efforts will be consistent with and dependent upon its internal risk analyses.
- 4) Notify (or require the applicable Participant to notify) the Individual(s) and any applicable regulatory agencies as required by federal, state and local laws and regulations, unless a law enforcement agency determines that such notification would negatively impact a criminal investigation.
- 5) Maintain a record of the actual or suspected breach, the investigation, determination and outcome.