

One Health Record®

Alabama's Health Information Exchange Policy Manual¹



(Effective October 1, 2023)

¹ Compliance with these policies and procedures is required for participation in Alabama's Health Information Exchange



One Health Record®

Alabama Health Information Exchange Policy Notice

These policies and procedures **do not supplant nor preempt** any federal or state laws applicable to health care providers or other entities.

Following these policies and procedures **does not protect** a Participant or Authorized Users o from liability under applicable law.

One Health Record® is intended to be used as an information gathering tool to aid health care Providers, other Participants, and Authorized Users.

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 nor guarantee** the accuracy or completeness of the information made available from Participants through its operations.

Quality of Information

Each Participant is responsible for maintaining the **quality** and **security** of information entered into Participant's Electronic Medical Records and made available to other Participants through AHIE.

AHIE is not responsible for verifying or correcting any information made available by Participant through AHIE.

Table of Contents

Background & Purpose	6
AHIE Policy Manual Introduction	7
Definitions	9
Duties of the AHIE Governing Authority	22
Obligations of the AHIE	23
Participant Obligations and Policies – Introduction	24
Participant and Authorized User On-Boarding	25
Compliance with Law and Policy	27
Participant Notice of Privacy Practices	29
Individual Participation and Choice	30
Automatic Inclusion	30
Opt-Out Procedures	31
Opt-out Option under One Health Record®	31
Revocation of Opt-Out Option	31
Participant’s Maintenance of Opt-Out Documentation	32
Prohibition of Withholding Care Based on Opt-Out Status	32
Permitted Purposes: Use, Disclosure, & Requests	33
Provider Permitted Uses and Accessible Data	33
Health Plan Permitted Uses and Accessible Data	34
Public Health Authority Permitted Use and Accessible Data	35
AHIE Permitted Uses	35
Requests for Health Information	36
Compliance with AHIE and Participant Internal Policies	36
Limitations	37
Permitted Use Case Descriptions and Examples	38

Information Subject to Special Protection	42
Sensitive Information	42
Part 2 Information	42
HIPAA Restricted Self-Pay Information	43
Compliance with Applicable Law and AHIE Policies	43
Minimum Necessary Information	44
Access to AHIE: Participant Requirements and Responsibilities	45
Access Limitations	45
Workforce Training	45
Access Security	46
Breach Prevention, Mitigation, and Notification	47
Reasonable Safeguards	47
Breach Mitigation	47
Identify, Respond to, and Document Breaches	48
Breach Reporting	48
Compliance with Audit Requests	48
AHIE Breach Response	48
Compliance with HIPAA	49
Enforcement	49
Rights of Individual Regarding Health Information	50
Right to Access	50
Right to Amend	50
Right to an Accounting of Disclosures	51
Complaints	52
Complaint Management	52
Documentation of Complaints	52
Nature of Complaints	53

Prohibition of Information Blocking	54
Definition	54
Compliance with the Information Blocking Rule	54
Information Blocking Complaint Management	55
Appendix A Regulatory Foundation	56

Background and Purpose

In 2010, One Health Record® was created as the foundational component of the Alabama Health Information Exchange network for providing a safe, secure effective, and universal platform for sharing health information.

Currently, One Health Record® is administered and managed by the Alabama Medicaid Agency.

Now, as then, the purpose of the AHIE network in the form of One Health Record®, is to dramatically improve the safety, efficiency, and quality of health care available to the residents of Alabama.

Utilizing and improving health information technology and interoperability, affirms Alabama's commitment to the health and well-being of its citizens. .

The AHIE Policy Manual

Introduction

This Alabama Health Information Exchange Policy Manual (AHIE Policy Manual) includes the documents approved by the Governing Authority and identifies the policies and procedures necessary for successful participation in the One Health Record® system. These policies establish baseline operating rules for One Health Record® as the provider of the AHIE services, and for AHIE Participants, and Authorized Users of the AHIE network.

The AHIE Manual includes definitions for terms used throughout AHIE documents, as well as AHIE Performance and Service Specifications, AHIE Policies and Procedures, the Participation Agreement, the Business Associate Agreement, and any other documents approved by the Governing Authority of One Health Record®.

Each Participant and Authorized User is contractually bound to abide by the AHIE Policy Manual. The Governing Authority shall review and may amend the AHIE Policy Manual from time to time as provided for in the Participation Agreement.

The policies contained in this AHIE Policy Manual provide basic, minimum policy requirements for Participants who will be engaged in the exchange of electronic health information through the AHIE network following the execution of both the AHIE Data Use and Reciprocal Sharing Agreement (DURSA), also called the *Participation Agreement* and *Business Associate Agreement (BAA)*.

The policies included here apply to all Participants and Authorized Users accessing the Alabama Health Information Exchange and are intended to ensure the Alabama HIE is used in an effective, efficient, ethical, and lawful manner.

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.

A Participant's failure to comply with AHIE policies and procedures in this Manual and associated documents constitutes a breach of the AHIE Participation Agreement/DURSA and may result in termination of the Agreement, loss of access privileges to the AHIE

network, or financial penalties as discussed in the AHIE Participation Agreement and herein.

These policies may be revised and updated periodically in accordance with the Participation Agreement, in response to changes in applicable laws and regulations, changes in technology and standards, or other factors affecting the governance and operation of the AHIE network.

The current version of the AHIE Policy Manual is available on the One Health Record® website at www.onehealthrecord.alabama.gov. Each Participant is responsible for ensuring it obtains, and is in compliance with, the most recent version of these policies and procedures.

Any suggested additions or changes to these policies should be submitted to the AHIE Executive Director and the Governing Authority for consideration.

Definitions

The following definitions are provided to facilitate a common understanding and consistent application of AHIE policies among Participants and Authorized Users by providing a single reference for defined terms used throughout the AHIE Policy Manual, the AHIE Participant Agreement, (also called the Data Use and Reciprocal Support Agreement or DURSA), as well as the Business Associate Agreement (BAA) between Participant and AHIE.

Unless otherwise specified, all capitalized terms used in this AHIE Policy Manual shall have the same meaning as set forth in the laws and regulations identified in Appendix A of this AHIE Policy Manual titled, *Regulatory Foundation*.

Any change in law that modifies a definition or alters the regulatory citation of a definition, shall be deemed incorporated into this AHIE Policy Manual and associated documents.

Access

The ability or means necessary to make electronic health information available for exchange or use. [45 CFR § 171.102]

Actor

A healthcare provider, health IT developer of certified health IT, health information network or health information exchange (HIE), all as defined by the Information Blocking Rule. [45 CFR § 171.102]

AHIE

The Alabama Health Information Exchange network, also known as One Health Record® that provides the core system components including a Master Person Index (eMPI).

AHIE Interoperability Specifications

The AHIE Implementation Approach and Interface Specifications as referenced in the AHIE Policy Manual and as amended from time to time.

AHIE Policy Manual

The documents approved by the Governing Authority including the definitions, policies, procedures, and all content herein, AHIE Performance and Service Specifications, the Participation Agreement, also called the Data Use and Reciprocal Support Agreement or DURSA 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.

AHIE Policies and Procedures

The policies and procedures adopted by the Governing Authority that describe management, operation, and participation in the AHIE network and included in the AHIE Policy Manual

Applicable Law

Federal, state, or local statutes and regulations applicable to the AHIE - One Health Record®, Participants, Authorized Users or other individuals who access Data through AHIE - One Health Record®

Audit

A review and examination of records (including logs), and/or other activities to ensure compliance with the Participation Agreement and the AHIE Policy Manual and to ensure the accuracy of the data transmission and conversion of data at the Integration Point. This review can be manual, automated or a combination of both.

Audit Host

Any designee the AHIE contracts with to provide the audit services to support the AHIE and the System.

Authorization

Permission obtained from an Individual that permits the use or disclose that Individual's protected health information to someone else for a purpose that would otherwise not be permitted by the HIPAA. To be valid, an Authorization must include the content requirements of 45 CFR § 164.508(b)

Authorized User

An individual Participant or an individual Participant User designated to use AHIE Services on behalf of the Participant.

Authorized Users receive their rights to use the Services by registering as Participants themselves or through an organization that registers as a Participant and designates individuals to be authorized to use the Services on the Participant's behalf.

An Authorized User may be:

- An individual physician who registers as a Participant
- A member of that physician's office staff designated by the physician
- A hospital employee and/or medical staff authorized by the hospital to act as Authorized Users under the hospital's registration as a Participant.

Breach

The acquisition, access, use, or disclosure of Data in a manner not permitted under the Privacy Rule which compromises the security or privacy of the Data consistent with the definition as set forth in 45 CFR § 164.402.

Business Associate

A person or entity that performs certain functions or activities involving the use or disclosure of protected health information on behalf of, or provides services to, a covered entity consistent with the definition as set forth in 45 CFR § 160.103

Business Associate Agreement (BAA)

A contract between a covered entity and a business associate that meets the content requirements set forth in 45 CFR § 164.504(e)(1)-(5)

Clinical Data Repository (CDR)

An aggregation of granular patient-centric health data usually collected from multiple-source IT systems and intended to support multiple permitted uses of the Data.

Collect/Collection

The acquisition or receipt of information, including PHI and PII.

Core Services

Shall be limited to the following services provided by One Health Record®

- Master Patient Index (MPI)
- Provider Directory
- Record Locator Service (RLS)
- Terminology Standards and Services
- Public Key Infrastructure (PKI) certificate-based encryption and authentication
- Audit/Log document tracking
- Clinical Data Repository
- Fast Healthcare Interoperable Resource (FHIR) and Patient Access mobile app
- ehealth Exchange (eHX) or Qualified Health Information Network (QHIN) Gateway

Consent

As the term is defined in the context of 45 CFR § 164.506 and §164.508

Corrective Measures or Mitigation

Actions taken to address a security breach or privacy violation, with the intent to counteract the breach or violation and reduce future risks.

Covered Entity

As the term is defined in 45 CFR § 164.103

The 21st Century Cures Act

The enacted Federal requirements passed by United States Congress for health information exchange and interoperability

Data

Information requested or sent by a Participant to another Participant through the AHIE network. This includes, but is not limited to, PHI, de-identified data, pseudonymized data and metadata.

Data Aggregation

As the term is defined in 45 CFR § 164.501.

De-identified Data

Health information, or Data, that does not identify an Individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an Individual. The standards for de-identifying Data are set forth in 45 CFR § 164.514(a) and § 164.514 (b)

Designated Record Set

As the term is defined in 45 CFR §164.501

Disclose/Disclosure

The release, transfer, provision of access to, or divulging in any other manner, information outside of the entity holding the information.

DURSA

Data Use and Reciprocal Support Agreement, also known as the *Participation Agreement*, 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®

Effective Date

The date on which a Participant executes the DURSA/Participation Agreement.

eHealth Exchange (eHX)

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. This organization was formally known as the Nationwide Health Information Exchange or NHIN.

Electronic Health Record (EHR)

An electronic record of an Individual's health-related information that is created, gathered, managed, and consulted by authorized health care clinicians and staff as set forth in Subtitle D-Privacy, Section 13400(5) of the HITECH Act.

Electronic Protected Health Information (EPHI)

Individually identifiable health information

- Transmitted by electronic media;
- Maintained in electronic media; and including without limitation,
- Any EPHI provided by a Covered Entity or created or received by a Business Associate on behalf of a Covered Entity.

Executive Director

The Executive Director of the AHIE.

Governing Authority

The Alabama Medicaid Agency, as vested by the State of Alabama, 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 network pursuant to legislation.

Health Care Operations

Certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment, such as: patient safety activities, population-based activities relating to improving health or reducing health care costs, case management and care coordination, evaluation of the competence/qualifications of health professionals, business planning and development, and other administrative and management activities. [45 CFR §164.501]

Health Information

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 and alone or in combination with other information identifies the Individual.

Health Care Organization (HCO)

Health care providers, public health agencies, payers, and other entities offering patient engagement services, such as Patient Health Records.

Health Information Exchange (HIE)

The use of technology, facilitated by applied standards, that provides the capability to electronically move clinical information among disparate healthcare information systems among a variety of stakeholders, including healthcare providers, while maintaining the integrity and meaning of the information being exchanged. The purpose of health information exchange is to facilitate access to, and retrieval of, clinical data to provide safe, timely, efficient, effective and equitable patient-centered care. For the purposes of the Information Blocking Policy, HIE shall have the same meaning as set forth in 45 CFR § 171.102.

Health Information Organization (HIO)

An organization that oversees and governs the exchange of health-related information locally or regionally among health care organizations according to nationally recognized standards.

HIPAA

The Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, as amended, and related regulations [45 CFR §§160-164].

HIPAA-Restricted Self-Pay Data

Data pertaining to a healthcare item or service for which an Individual fully pays out-of-pocket and which the Individual requests not be disclosed to a health plan.

HITECH

The Health Information Technology for Economic and Clinical Health Act, including any and all amendments, 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 a HIE with respect to HIPAA.

Individual

The person who is the subject of the health information, but also includes a person who qualifies as an authorized representative of the Individual in accordance with legal requirements, whose PHI may be transmitted by Participants via One Health Record®.

Individually Identifiable Health Information

Information 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 health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and
- Identifies the Individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. [45 CFR §164.103]

Information Blocking

A practice that, except as required by law or covered by an exception set forth in subpart B or subpart C of 45 CFR § 171 (*Information Blocking*), is likely to interfere with the access, exchange, or use of electronic health information, and the perpetrator knows the practice is likely to interfere as stated above, and further defined in 45 CFR § 171.103. [until oct 1, 2023 the information that may be interfered with is limited to the USCDI standard at § 170.213]

Integration Point

The technical mechanism or service point that retains or furnishes a data source's patient demographic and clinical data, which identifies the data to a statewide Enterprise Master Patient Index, and allows for a real time sharing of clinical information (based on role based access controls) from connected electronic data systems or services.

Interfere “with” or Interference

To prevent, materially discourage, or otherwise inhibit [45 CFR § 171.102]

Interoperability

Making health data accessible for both patients and providers seamlessly across geographic boundaries, thereby increasing the use of the electronic health data to improve outcomes, and potentially optimize the health of Individuals and populations.

Monitor

An on-going 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.

Notice or Notify

A written communication sent to the appropriate Participant's representative at the address listed in the Participation Agreement or to the Governing Authority.

ONC

The Office of the National Coordinator for Health Information Technology in the Office of the Secretary, U.S. Department of Health and Human Services.

One Health Record®

Alabama's Health Information Exchange services, platform, and health information network (also referenced as AHIE)

Optional Services

Includes the services that AHIE may provide to Participants who choose to contract and pay for such services in addition to the Core Services covered under the terms of the Participation Agreement: Analytical Tools and other optional services.

Opt-Out

An Individual's choice not to have his or her electronic health records accessed or made available through One Health Record®.

ORS

The Office of Research and Statistics at the State Budget and Control Board

Part 2

Title 42 of the Code of Federal Regulations (CFR) Part 2: Confidentiality of Substance Use Disorder Patient Records. Collectively refers to 42 U.S.C. § 290 dd-2 and its implementing regulations.

Part 2 Data

Information related to substance use disorder treatment or mental health treatment that is subject to and protected by Part 2 regulations.

Participant

A person or a legal entity other than the Governing Authority that is a signatory to the DURSA or Participation Agreement with One Health Record® and is registered and authorized to access the AHIE.

If the entity or Health Care Operations department within which the individual practices signs a Participation Agreement, the individual is not required to sign a separate Participation Agreement, but must sign a Participant (Authorized) User Agreement.

For the purpose of this part, “**eligible individuals**” are health care providers licensed in Alabama and providing health care services within their statutory scope of practice, including, but not limited to 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, tele-monitoring providers, pharmacies, and governmental agencies involved in healthcare.

Participation Agreement

The Data Use and Reciprocal Support Agreement and all amendments addendum, attachments, exhibits, or statements of work thereto that a Participant agrees to and signs as a condition of joining the AHIE, which establishes the Participant’s obligations and responsibilities related to disclosing, accessing, exchanging and using Data through the AHIE.

Patient Access

The ability of an Individuals who is the subject of health records to view, copy, or correct information in those records.

Payment

Shall have the meaning set forth at 45 CFR § 164.501

Permitted Purposes

Those reasons defined within federal and/or state law or AHIE policies for which Participants and Authorized Users may legitimately access, use, and/or disclose Data through the AHIE.

Personally Identifiable Information (PII)

Information that identifies the Individual whether 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, driver's license number, social security number, banking information, or claims information.

Persons and Entities

Health care professionals, partnerships, proprietorships, corporations and other types of organizations and their agents when acting on their behalf.

Privacy

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.

Privacy Rule

The Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule), 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 The Cures Act and HITECH.

Protected Health Information (PHI)

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 consistent with the definition set forth in 45 CFR § 160.103, including, without limitation, any PHI provided by or received by a Participant User. Unless otherwise stated in the Participation Agreement or this AHIE Policy Manual, any provision, restriction, or obligation in the Participation Agreement related to the use of PHI shall apply equally to ePHI.

Recipient

A Participant who receives PHI and PII through the AHIE network.

Record Locator Service (RLS)

The system that identifies and links Individuals with their data across the linked continuum of care.

Regional Health Information Organization (RHIO)

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.

Required By Law

A mandate contained in law that compels an entity to make a use or disclosure of protected health information that is enforceable in a court of law and consistent with the term's definition set forth in 45 CFR § 164.103, and any additional requirements created under applicable Federal and/or State law.

Safeguards

Physical, technological, and administrative policies, precautions, and technical standards that control the access, use, and disclosure of PHI and PII and other related data.

Secretary

The Secretary of the United States Department of Health and Human Services or his designee.

Security

Utilization of physical, technological, and administrative safeguards to protect the integrity, confidentiality, and availability of individually identifiable health information

Security Incident

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 CFR § 164.304.

Security Rule

The Security Standards for the Protection of Electronic Protected Health Information in 45 CFR §§ 160 and 164.

Sensitive Information

Individually identifiable information, which if lost, compromised, misused, disclosed or without authorization is accessed or modified, or otherwise could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual who is the subject of the information.²

System

The AHIE's internet-based, authenticated, peer-to-peer computer system and search engine for patient health, demographic, and related information that assists Participants and/or Authorized 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.

Transparency

Making available to the public, in a reliable and understandable manner, information on the health care system's quality, efficiency, cost, and consumer satisfaction

Treatment

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 an Individual; or the referral of an Individual for health care from one health care provider or another, and consistent with meaning set forth in 45 CFR § 164.501.

Treatment Relationship – Direct

A treatment relationship between a healthcare Provider (Participant User) and the Individual being treated. A Direct Treatment Relationship includes an emergency treatment relationship formed due an Individual's emergent condition and requiring immediate treatment by a healthcare Provider (Participant User).

Treatment Relationship–Indirect

A treatment relationship between an Individual and a health care Provider (Participant User) in which:

² See Information Subject to Special Protection p. 42

- The health care Provider (Participant User) delivers health care to the Individual based on the orders of another health care Provider; and
- The health care Provider (Participant User) typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care Provider, who provides the services or products or reports to the Individual.

Unsecured PHI

PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption technologies or methods of physical destruction approved by the Secretary of HHS pursuant to § 13402 of HITECH.

Use

With respect to individually identifiable health information, the employment, application, utilization, examination, or analysis of PHI and PII.

Workforce Member

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.

AHIE Policy ## 001

Effective Date: October 1, 2023

Duties of the AHIE Governing Authority**Purpose**

To establish duties of the Governing Authority of the AHIE

Policy

The Governing Authority shall have the following duties:

1. Provide policy direction and operational guidance for the AHIE Executive Director who shall serve at the pleasure of the Governing Authority;
2. Oversee the development, implementation, and operation of AHIE in compliance with all applicable state and federal requirements;
3. Establish a legal and policy framework for the operation and financial stability of AHIE, consistent with state and federal requirements;
4. Develop, implement, review and revise strategic objectives and operational plans for the AHIE as approved by the AHIE Governing Authority. ;
5. Develop and implement policies and procedures governing the AHIE that are consistent with state and federal law, and include the right of patients to opt out of having their PHI exchanged through the AHIE;
6. Develop the necessary agreements to facilitate the secure exchange of electronic health information through the AHIE and among all Participants and/or trading partners; and
7. Encourage all applicable state agencies to participate in the AHIE.

AHIE Policy ## 002

Effective Date: October 1, 2023

Obligations of the AHIE**Purpose**

To establish the obligations of the Alabama Health Information Exchange as implemented through One Health Record®

Policy

One Health Record® shall:

1. Comply with all applicable federal, state, and local laws and regulations, including but not limited to HIPAA and 21st Century Cures Act, , as they pertain to PHI exchanged electronically through the AHIE.
2. Work toward establishing a protocol to provide Individuals with a simple and timely means to access and obtain their PHI stored by AHIE in a readable form and format.
3. Work toward establishing a protocol 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. Work toward establishing a protocol to grant Individuals the ability to request and review documentation to determine who accessed their information through AHIE.
5. 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.
6. Where applicable, require a Business Associate Agreement be entered into by and between One Health Record® and the Participant.

PARTICIPANT OBLIGATIONS AND POLICIES

The following policies serve to establish the obligations of Participants beginning with the required agreements and associated documents necessary for connection to the Alabama HIE network, receiving and maintaining necessary access to the information exchanged through One Health Record®.

Understanding and abiding by these policies facilitates Participant compliance with federal and state law applicable to the exchange of individually identifiable information thereby assisting Participants in the care of the Individuals served.

AHIE Policy ## 003

Effective Date: October 1, 2023

Participant and Authorized User On-Boarding

Purpose

To define the Agreements and necessary procedures required of a health care Provider or other eligible organization to become a Participant in the Alabama HIE and appoint Authorized Users.

Policy³

Prior to beginning electronic exchange of data through One Health Record®, each Participant must execute a DURSA (Participation Agreement) with the AHIE, establishing the mutual responsibilities of One Health Record® and the Participant;

Prior to beginning electronic exchange of data through One Health Record®, each Participant must execute a valid HIPAA Business Associate Agreement with the AHIE;

Participant shall continuously comply with all applicable One Health Record® Policies and Procedures.

Because AHIE may revise these policies due to changes in law, regulations or technology, each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of the AHIE Policy Manual.

Participant is responsible for the development, documentation, and implementation of internal policies that address the privacy and security of PHI and PII.

Participant is responsible for training its workforce as to its internal policies and AHIE policies related to PHI and PII.

In the event of a conflict between One Health Record® Policies and Procedures and the Participant's own policies and procedures, the Participant shall comply with the policy that more stringent in the application of privacy and security protections to individually identifiable information.

³ Certain content in this policy are included in more detail in subsequent policies.

Each Participant shall provide a name and contact information for a designated point person who will be the primary responsible party for matters related to the AHIE.

Participants shall identify the members of its workforce that are to be designated Authorized Users,

Participants shall monitor its Authorized Users to ensure compliance with Participant's internal policies, AHIE policies, and applicable law.

Participants are responsible for communicating with One Health Record® when there is any change in an Authorized User's role or need for access to the AHIE.

AHIE Policy ## 004

Effective Date: October 1, 2023

Compliance with Law and Policy**Purpose**

To ensure each Participant and Authorized User shall, at all times, comply with AHIE policies and all applicable federal and state laws and regulations, including but not limited to, those protecting the privacy and security of individually identifiable health information and the rights of those who are the subject of the information.

Policy**Compliance with Law and Policy**

In addition to complying with the requirements established in the AHIE Participation Agreement (DURSA), Participants shall comply with all applicable federal and state laws and regulations, including, but not limited to, HIPAA, The 21st Century Cures Act, HITECH, and Interoperability and Patient Access Rule, as they pertain to PHI exchanged electronically through the AHIE.

Each Participant and Authorized User shall use reasonable efforts to stay abreast of any changes or updates in law or guidance, and changes in interpretations of all applicable federal and state laws and regulations that may affect the Participant's or Authorized User's use and disclosure of data.

Participants and Authorized Users will be provided reasonable notice of any material changes in AHIE policy.

The most current version of Participant policies will be made available to all Participants and Authorized Users through the One Health Record® website and/or upon request to the AHIE.

Participants and Authorized Users are responsible for ensuring compliance with the most recent version of AHIE policies.

Participant's Policies

Participant is responsible for ensuring it has developed and implemented appropriate internal policies and procedures to ensure Authorized Users comply with applicable laws and AHIE policies.

Participant is responsible for revising existing internal policies or developing new internal policies necessitated by changes in applicable laws and regulations to ensure it has the requisite, appropriate, and necessary internal policies in place to maintain compliance with such laws and regulations.

Participant is responsible for monitoring State laws that may necessitate a change in its internal policies related to the use and disclosure of information, including revising internal policies to comply with State laws that may be more stringent than federal law related to the use and disclosure of PHI and PII.

Participants must be aware of any State law that provides special protections for certain types of health information, such as HIV status or Substance Use Disorder.⁴

Participants internal policies must allow Participant to be compliant with the more stringent law, if federal and state laws have contradictory requirements.

⁴ See AHIE Policy ## Special Protections

AHIE Policy ## 005

Effective Date: October 1, 2023

Participant Notice of Privacy Practices

Purpose

To ensure the Participant provides Individuals with a Notice of Privacy Practices (NPP) that adequately addresses the Participant's practices with respect to the exchange of data through the AHIE

Policy

A Participant who is a Covered Entities as defined in 45 CFR §160.103, shall develop, maintain, and distribute, a NPP that complies with the requirements of the HIPAA Privacy Rule, HITECH, the 21st Century Cures Act, and both the AHIE's and Participant's internal policies, as applicable

The Participant's Notice of Privacy Practices shall:

- Include all required content as set forth under HIPAA at 45 CFR § 164.520(b)
- Describe to Individuals the Permitted Purposes for which PHI may be collected, used, and/or disclosed without Individual authorization, as part of Participant's treatment, payment or healthcare operations activities.
- Be distributed as specified by HIPAA in 45 CFR § 164.520 (c)

Participants that are required to provide a Notice of Privacy Practices to Individuals shall implement internal policies and procedures governing the maintenance and distribution of the NPP

Participants shall be open and transparent with Individuals about Participant's privacy and security practices, including the sharing of Data through One Health Record®.⁵

⁵See Policy: Individual Participation and Choice that addresses Individual's right to Op-Out of PHI exchange.

AHIE Policy ## 006

Effective Date: October 1, 2023

Individual Participation and Choice**Purpose**

To establish the Participant's obligation to notify Individuals of Participant's exchange of PHI through the AHIE and the Individual's right to "Opt-Out" of this exchange.

Policy**Automatic Inclusion**

Participant will ensure that Individuals have the opportunity to review Participant's Notice of Privacy Practices that adequately addresses the Participant's specific privacy practices with respect to the exchange of information through the AHIE.

Participant's Notice of Privacy Practices shall advise Individuals that Participant may request, use and/or disclose Protected Health Information through the AHIE without an Individual's Authorization for Permitted Uses, such as treatment, payment and healthcare operations.

The exchange of PHI through One Health Record® does not require an authorization from the Individual so long as the use or disclosure is for a Permitted Purpose.

[45 CFR § 164.502(a)(1); 45 CFR § 164.506(c)]

Any data which is available through a Participant may be made available through the AHIE provided that an Individual has not opted-out of participating in the AHIE.

That data is available through the AHIE does NOT automatically permit access to that data by all Participants and Authorized Users.

Only Participants and Authorized Users may access the data and only for a Permitted Use, not a Prohibited Use, and in accordance with law and the AHIE policies.

Opt-Out Procedures

Even though disclosure of PHI through One Health Record® for Permitted Purposes is allowed without an Individual's authorization, the Participant shall provide Individuals the option to choose *not* to participate in the electronic sharing of his or her protected health information through One Health Record®.

Opt-out Option under One Health Record®

Participant shall implement processes to allow an Individual to Opt-Out of participation in the electronic sharing of his or her PHI through One Health Record®.

If an Individual chooses to opt-out of One Health Record® information regarding that Individual will not be included, made available, nor exchanged through, the 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 the AHIE is "an all or none" choice. If an Individual chooses to Opt-Out, no information regarding the Individual will be exchanged or made available from any Participant unless required by law.

Participant shall ensure that an Individual's choice to opt-out is durable and revocable, made in writing, signed and dated. Similarly, the choice to revoke an opt-out decision must be in writing. The form and manner of the Opt-Out may be determined by the Participant.

Once an Individual provides to the Participant a written and signed decision to Opt-Out, 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. The Participant shall notify One Health Record® of an Individual's decision to opt-out. Notification shall be made via the AHIE Portal where the decision is logged and confirmed by clicking the "opt-out" button. At this point, Participant has fulfilled its obligations in regards to the Individual's opt-out decision.

The "opt out" shall stand through multiple admissions/visits unless revoked by the Individual.

Participant is not required to give additional notice to the Individual once that Individual has chosen to opt out.

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.

Participant's Maintenance of Opt-Out Documentation

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

Prohibition of 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 his or her information exchanged electronically through One Health Record® and shall make every reasonable effort to avoid any adverse impact on the quality of care.

AHIE Policy ## 007

Effective Date: October 1, 2023

Permitted Purposes: Use, Disclosure, and Requests for Protected Health Information

Purpose

To set forth the Permitted Purposes for which health information through AHIE may be used, disclosed or requested by Participants and Authorized Users and by the AHIE.

Policy

Use and Disclosure of Health Information through AHIE

Participants and Authorized Users shall only use and disclose health information for Permitted Purposes and in compliance with all applicable federal, state, and local laws and AHIE policies.

Participants and Authorized Users are prohibited from using or disclosing health information for unlawful or discriminatory purposes.

Provider Permitted Use

Participants that are Healthcare Providers (or Business Associates acting on behalf of Healthcare Providers) may access the Data through the AHIE for the following Permitted Uses (and subject to the limitations required by Applicable Law or this policy):

- **Treatment** (including care coordination, case management and transition of care planning);
- **Payment**; and
- **Limited Healthcare Operations** (including population health activities), so long as:
 - The Healthcare Provider has (or had) an established relationship with the individual who is the subject of the Data and the Data pertains to that relationship; and
 - The Healthcare Provider is a HIPAA Covered Entity.

Individuals for Whom Data May Be Accessed by Provider

Treatment and Payment - Access is permitted for permitted for Data of Individuals who are:

- Current patients of the Healthcare Provider;
- Prospective patients with whom the Healthcare Provider is expected to establish a treatment relationship (for example, an individual who is scheduled for an upcoming appointment or who has been assigned to the Healthcare Provider by a Health Plan); and
- Past patients for whom the Healthcare Provider is transitioning to a new Healthcare Provider (for example, individuals who have an outstanding payment obligation to the Healthcare Provider that is transitioning care).

Limited Healthcare Operations - Access is permitted for Data of Individuals who are current or past patients of the Healthcare Provider.

Health Plan Permitted Use

Participants that are Health Plans (or Business Associates acting on behalf of Health Plans) may access the Data through the AHIE for the following Permitted Uses (and subject to the limitations required by Applicable Law and this policy):

- **Payment;** and
- **Limited Healthcare Operations** (including care coordination, case management, transition of care planning, and population health activities), so long as:
 - The Health Plan has (or had) an established relationship with the Individual who is the subject of the Data and the Data pertains to that relationship; and
 - The Health Plan is a HIPAA Covered Entity.

Individuals for Whom Data May Be Accessed

Access is permitted for Data of Individuals who are

- Currently enrolled members with the Health Plan and
- Past members for whom the Health Plan is transitioning to a new Health Plan.
- Prospective members seeking to enroll in the Health Plan if necessary, for Payment purposes.

Public Health Authority Permitted Use Cases and Requirements

Limited Public Health Investigations

A Public Health Authority that is a Participant may access Data for a Limited Public Health Investigation. This use case is conditioned on there being adequate technical and/or administrative procedures in place to provide access in compliance with Applicable Law.

AHIE will not give a Public Health Authority direct access to the AHIE for a Limited Public Health Investigation until this legal precondition is satisfied.

Individuals for Whom Data May Be Accessed

Access is permitted for Data of Individuals who are the subject of a Limited Public Health Investigation.

AHIE Permitted Uses

AHIE is a Business Associate of its Participants.

AHIE may not use or disclose Data in a manner prohibited by Applicable Law.

AHIE may access, use and disclose Data for the following Permitted Uses:

- As required by law;
- As necessary to perform services under the Participation Agreement and to assist Participants (and Participants' Business Associates) in the Permitted Uses;
- As directed in writing by the Participant that provided the Data to AHIE;
- To provide access to Authorized Requestors such as Insurance Companies, if AHIE has the necessary technical and administrative processes in place to support Authorized Requestors' access in accordance with Applicable Law and healthcare industry standard security practices;
- To conduct public health reporting
- To facilitate health information exchange through trusted networks for any of the Permitted Uses set forth in this policy, including (but not limited to) Treatment, Payment, Limited Healthcare Operations, public health reporting, and Limited Public Health Investigations;
- For AHIE's own management and administration or to carry out its legal responsibilities, including (but not limited to) audit, legal defense and liability, record keeping, and similar obligations.

Requests for Health Information

Participant, including its Authorized Users, may request health information through AHIE only for Permitted Purposes.

A Participant shall request health information through AHIE only to the extent necessary⁶ and only for Permitted Purposes.

Information received in response to a request must not be disclosed to any third party for a non-Permitted Purpose unless required by applicable state or federal laws.

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 entity 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 entity.

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.

Compliance with AHIE and Participant's Internal Policies.

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

Once Data from the AHIE is accessed by a Participant for a Permitted Use as set forth in this policy, and incorporated into a Participant's electronic systems, the Participant may use or disclose such Data in accordance with Applicable Law and Participant's internal policies.

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

⁶ See AHIE Policy: Minimum Necessary

Limitations

Multi-party trust arrangements

AHIE participates in multi-party trust arrangements with other HIEs, federal agencies, and other entities and organizations that participate in electronic health information exchange for purposes permitted by applicable law. Participation in Trusted HIE Connections promotes interoperability by facilitating secure access to health information when and where it is needed to support patient care, Healthcare Operations, and public health activities.

For example, AHIE participates in eHealth Exchange—a data sharing network of governmental and non-governmental exchange partners that share information for specific purposes. When accessing Data through a trusted network, Participant must comply with any requirements applicable to that trusted HIE connection, such as limitations on the purposes for which Data may be accessed.

Permitted Use Case Examples

Permitted Use Case 1: Treatment

Statutory and regulatory basis: Treatment - 45 CFR §164.501-506

Description of use

AHIE Data may be used by Healthcare Providers to provide Treatment to Individuals.

Treatment is defined as “the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a Patient, or the referral of a Patient from one health care provider to another.” 45 CFR § 164.501.

Examples of Permitted Use for Treatment by a Authorized User:

- Outpatient clinical Provider accesses Data in connection with an Individual’s follow-up office visit.
- A care coordination team reviews Data on behalf of those Participants contributing such Data to determine whether hospitalized Individual is a candidate for care coordination intervention.
- Authorized Users and Participants view Medicaid prescription data.
- Emergency room physician reviews Data when Individual presents at ED.
- Managed care organization’s care coordinator, in collaboration with members’ physician(s) and/or other care coordinators, accesses AHIE Data in developing care coordination plan for MCO member. (Managed Care personnel performing administrative functions for the payor such as cost evaluation, will have access to the minimum necessary PHI in order to perform those functions).
- Care coordination team records medication reconciliation and care coordination activities in HIE that is viewable by other treating clinicians.

Permitted Use Case 2: Population Health and ACO – Notice to Primary Care Practice

Statutory and regulatory basis: Health Care Operations & Treatment- 45 CFR §§ 164.501-506

Description of use

An HIE is developing an Accountable Care Registry (ACR) that tracks patients by primary care practice and payer.

The ACR enables the creation of various reports of data contained in the HIE to corresponding practices and payers. The ACR is created and maintained for each participating practice based on multiple Data sources, including practices' patient records, patient capitation lists from MCOs, and hospital records of Patient self-identification.

The ACR is updated monthly.

The first application of the ACR is the development of daily reports by the HIE, as a Business Associate of and on behalf of AHIE Participants, of attributed patients who have been seen in the Emergency Department (ED) or admitted to the hospital.

Patients at ABC Hospital Emergency Department who indicate that they do not want their hospital records shared are excluded from the daily report.

The Use Case may expand with additional Data to provide the practice or organization with reports to help manage targeted quality metrics such as routine mammograms and cervical cancer screenings, etc.

The ACR falls within Health Care Operations as a “population-based activity relating to improving health or reducing health care costs” and an integral part of “case management and care coordination.” The daily reports promote targeted care coordination for Patients who are at-risk of readmission and require prompt post-discharge follow-up care.

Examples of permitted use by Authorized User

- Primary care practice receives daily report of ED and inpatient admission and uses it to contact patient and hospital's clinical staff to coordinate care while in the hospital.
- Care coordination team working with a practice uses daily report to identify Patients to outreach and schedule follow-up appointments.

Permitted Use Case 3: Health Care Operations – Planning and Practice Improvement Activities

Statutory and regulatory basis: Health Care Operations - 45 CFR § 164.501-506

Description of use

The Medicaid Agency's Program Division use AHIE Data to better understand current health care utilization patterns, the frequency of various health conditions, and other important aspects of the local health care landscape for the purpose of improving health care operations at the practice and system level.

This information can be used for a wide range of planning activities, including segmenting Patient populations to better understand utilization patterns, identifying areas of high need to target new or existing interventions and resources, and performing exploratory analysis to look for opportunities for practice improvement.

As a Business Associate of Participants, the AHIE may aggregate data for the purpose of program evaluation and performance improvement activities. The AHIE measures hospital utilization and readmission, which is metric for evaluating the overall effectiveness of a particular intervention or for identifying those who respond well (or do not respond well) to an intervention in order to better understand its impact and improve its effectiveness. Additional clinical Data in the AHIE will enable more robust evaluation of outcomes and performance analysis.

Planning and practice improvement falls within first category of Health Care Operations (45 CFR § 164.501): “conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and Patients with information about treatment alternatives; and related functions that do not include treatment.

Examples of permitted use by Authorized User

Program staff use AHIE Data to analyze and segment a practice's Patient population based on frequency of ED and inpatient hospital utilization to:

- Understand need for differing levels of care coordination and follow-up appointments.
- Evaluate the impact of a clinical intervention (e.g. care coordination or Patient education) on hospital utilization.
- Report the financial impact of programs on hospital utilization.

AHIE Policy -## 008

Effective Date: October 1, 2023

Information Subject to Special Protection

Purpose

To ensure individually identifiable information subject to Special Protection (“Sensitive Information”) is used, disclosed, or requested only as allowed under applicable federal or state law.

Policy

Participant is responsible for identifying Sensitive Information that is subject to special protection under applicable federal and state laws and regulations *prior* to disclosing any information through AHIE.

Sensitive Information includes, but is not limited to, information related to:

- HIV/AIDS
- Sexually Transmitted Disease
- Substance Use Disorder Records
- Mental Illness/Behavioral Health
- Psychotherapy Notes (as defined in HIPAA)

Part 2 Data

Part 2 regulations give heightened privacy protections to Part 2 Data (substance use disorder and mental health information).

Participants are permitted to access Part 2 Data as follows:

- Consent - Participant is responsible for obtaining a written consent meeting all of the content requirements of Part 2 consent process, signed by the Individual who is the subject of the Data or the Individual’s legal representative.
- Medical Emergency - Provider Participants may access Part 2 Data through the AHIE for emergency Treatment purposes, but only to the extent necessary to meet a bona fide medical emergency in which the Individual’s prior consent cannot be obtained.

HIPAA Restricted Self-Pay Information

In addition to the sensitive information listed above, HIPAA gives Individuals the right to ask their healthcare providers **not to disclose** protected health information (PHI) to health plans, where Individuals have paid for healthcare services in full out-of-pocket and the PHI relates to those healthcare services. This data is referred to as HIPAA Restricted Self-Pay Information.

Healthcare Providers are required to honor this type of request. As detailed below, the Participant is responsible for acting on the request to prevent disclosure of this information.

Compliance with Applicable Law and AHIE Policies

Participant is responsible for complying with applicable laws and regulations including those that govern and require special protection of information in portions of Participant's electronic medical record system and the Participant's other systems that interact with AHIE.

Participant is responsible for complying with governing laws and regulations and AHIE policies for appropriately designating information that requires special protection under the law.

If deemed necessary or appropriate, Participant may withhold an Individual's sensitive information from AHIE if no statutory or regulatory requirement compels disclosure of the information.

If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing an Individual's sensitive information, the Participant shall ensure that it has obtained the required documentation or met the requisite conditions prior to the use or disclosure.

AHIE Policy -## 009

Effective Date: October 1, 2023

Minimum Necessary Information**Purpose**

To establish the applicability of the Minimum Necessary Rule⁷ to health information exchanged through the AHIE in compliance with the HIPAA Privacy Rule.

Policy

Participant shall maintain and comply with its own internal Minimum Necessary policy and procedure consistent with HIPAA's Minimum Necessary provisions, as well as comply with the related policies of the AHIE.

Compliance with Law and Policy

With regard to health information accessed, used, disclosed, and/or requested through the AHIE relative to a Permitted Purpose, and absent of an exception within HIPAA, Participant and Authorized Users shall:

- Access and/or request only the minimum amount of health information as is necessary
- Use only the minimum amount of health information as is necessary
- Limit access to, and sharing of, health information with those employees, agents, and contractors who need the information in connection with a duly assigned job function or duty

Exceptions

The Minimum Necessary standards do not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes
- Disclosures to the Individual who is the subject of the information
- Uses or disclosures made pursuant to an Individual's authorization
- Uses or disclosures required for compliance with the HIPAA Administrative Simplification Rules
- Disclosures to the Department of Health and Human Services when disclosure of information is required under the Privacy Rule for enforcement purposes
- Uses or disclosures that are required by other law

⁷ 45 CFR § 164.502(b) and § 164.514(d)

AHIE Policy -## 010

Effective Date: October 1, 2023

Access to AHIE: Participant Requirements and Responsibilities**Purpose**

To establish AHIE access requirements and the Participant's responsibility related to those requirements.

Policy

Participant shall ensure compliance with all applicable federal and state laws, regulations, and AHIE policies related to the provision, appropriate use, and monitoring of access to the AHIE.

Access Limitations

Participant shall:

- Limit AHIE Access to designated Workforce Members, agents, and/or contractors who have a valid, role-based need for access.
- Ensure access is limited to Permitted Purposes only.
- Ensure that access is consistent with AHIE Minimum Necessary policy.

Workforce Training

Participant shall develop and implement a training program for its Workforce Members, agents, and contractors designated by Participant to be Authorized Users. Participant shall ensure the training meets the standard and implementation requirements set forth in HIPAA,⁸ and other applicable federal and state law and One Health Record® policies.

Training shall include, but not be limited to:

- Detailed review of AHIE Policies and Procedures,
- The Privacy and Security of PHI as set forth in HIPAA, The 21st Century Cures Act, HITECH, and other applicable laws
- Access consistent with a Permitted Purposes
- Opt-Out Procedures
- Sanctions for violations of applicable federal and state law and AHIE policies regarding access, use, and disclosure of PHI/PII.

⁸ 45 CFR § 164.530(b) Training: Standard/Implementation

Participant Documentation of Training

Participant must document and maintain documentation of training for all Workforce Members, agents, and/or contractors granted AHIE access by Participant. Participant shall ensure that each trained Workforce Member, agent, and/or contractor signs an acknowledgement that

- Training has been received,
- Training included review of all AHIE policies and procedures, and
- The trainee will adhere to applicable laws and regulations and AHIE policies and procedures.

No Workforce Member, agent, or contractor shall be provided with AHIE access nor with a log-on identifier or passcode without first having been trained on AHIE Policies and Procedures, as set forth in this AHIE Policy Manual.

Access Security

Participant shall maintain the security of AHIE Access.

Participant shall ensure each Workforce Member, agent, and/or contractor designated by Participant for AHIE access is assigned a specific and distinct log-on identifier and private passcode that will be required for AHIE access.

Participant is responsible for maintaining the security of all log-on identifiers.

Participant 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 prohibit the sharing of log-on identifiers and passcodes, include a system for conducting internal audits to identify improper or unauthorized access and potential or in-fact breaches.

Such policies shall allow for immediate termination of access to AHIE in the event of improper use or breach.

AHIE Policy ## 011

Effective Date: October 1, 2023

Breach Prevention, Mitigation, and Notification**Purpose**

To promote breach prevention and establish breach reporting procedures and mitigation strategies in the event of a breach of the PHI/PII that are consistent with the Breach Notification Rule and the AHIE Participation Agreement/DURSA.

Policy

Participant and AHIE shall protect the confidentiality, integrity, and availability of PHI and PII.

Reasonable Safeguards

Participant shall implement and maintain reasonable administrative⁹, technical¹⁰, and physical¹¹ safeguards¹² to protect individually identifiable information.

The safeguards implemented by Participant shall include reasonable measures to minimize the risk of an unauthorized or inappropriate access, use, or disclosure of individually identifiable information. Managing risk appropriately will lessen the likelihood that a violation of federal and state laws and/or One Health Record® Policies.

Breach Mitigation

Participant shall comply with the Breach Notification Rule¹³ established in HIPAA and HITECH regarding a breach of unsecured PHI.

At a minimum Participant shall implement mitigation procedures for breaches.¹⁴

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, regulations, Participant policies, or One Health Record® Policies.

⁹ 45 CFR § 164.308

¹⁰ 45 CFR § 164.312

¹¹ 45 CFR § 164.310

¹² 45 CFR § 164.530(c)

¹³ 45 CFR §§ 164.400-414

¹⁴ 45 CFR § 164.530(f)

Identify, Respond to, and Document Breaches.¹⁵

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.

In addition, Participant shall have the following obligations to AHIE with regard to its security practices:

Breach Reporting

Participant shall report any breach and/or violation of the AHIE Policies and Procedures by Participant's Workforce, agents and/or contractors, regardless of any assessment of harm, to the Executive Director of 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.

Comply with Requests from AHIE for 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.

AHIE Breach Response¹⁶

In the event 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:

- Notify any Participants whose data is affected by the breach.
- 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.
- 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.
- 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.

¹⁵ 45 CFR § 164.308,(a)(6)

¹⁶ Obligations of the AHIE regarding a breach are also included in the Business Associate Agreement signed in conjunction with the DURSA by both the Participant and the AHIE.

- Maintain a record of the actual or suspected breach, the investigation, determination and outcome.

Compliance with HIPAA.

Any obligation of Participant to report certain actions and occurrences to AHIE as set forth in this AHIE Policy Manual and related Agreements and documents shall only apply if such action or occurrence involved a patient for which information was accessed through AHIE.

Except for Participant's obligations to report to AHIE as set forth in this AHIE Policy Manual and related Agreements and documents, nothing in these policies and procedures is intended to impose requirements on Participant in addition to Participant's existing duties under HIPAA, The Cures Act, HITECH and other applicable federal rules and regulations.

Enforcement

The Executive Director of the AHIE or his designee, in conjunction with the Governing Authority's Privacy Office, must investigate any report or complaint of a breach or inappropriate access, use, or disclosure of patient information exchanged through AHIE or for a violation of the AHIE Policy Manual. Following the investigation, the Executive Director will issue a letter of findings and appropriate sanctions as necessary.

AHIE Policy ## 012	Effective Date: October 1, 2023
Rights of Individual Regarding Individual's Health Information	

Purpose

To acknowledge and honor the rights of an Individual rights with respect to their own protected health information accessible through AHIE.

Policy

Participant shall acknowledge and appropriately facilitate the exercise of rights of an Individual with regard to the Individual's health information in accordance with HIPAA, HITECH, The 21st Century Cures Act, the Interoperability and Patient Access rule, and other applicable federal or state law.

Right to Access Health Information

Participant shall establish the internal policies and procedures for responding to requests from an Individual to access or receive a copy of that Individual's health information maintained in the Participant's electronic medical record.

Participant shall not access One Health Record® to pull or produce information shared by another Participant in response to an Individual's request for access to his/her health information.

Participant's response to an Individual's access request shall be limited to the information contained in the responding Participant's records maintained on the Individual.

Requests for access to health information that are made directly to AHIE will generally be directed to the Participant originating the health information.

Right to Request Amendment of Health Information

Participant shall afford Individuals the right to request an Amendment to health information maintained by the Participant in a Designated Record Set in accordance with HIPAA¹⁷, HITECH and other applicable laws.

If Participant accepts a requested amendment to an Individual's health information and such information was accessed and may have been relied upon or could foreseeable have been relied upon by other Participants in the AHIE to the detriment of the Individual,

¹⁷ 45 CFR §164.526

then Participant shall make reasonable efforts to inform such other Participants of the Amendment.

Right to an Accounting of Disclosures

Participant shall recognize an Individual's right to request and receive an accounting of disclosures of the Individual's health information consistent with the Accounting of Disclosure¹⁸ provisions of HIPAA.

Participant shall maintain documentation of disclosures of an Individual's health information other than those disclosures HIPAA expressly exempts from inclusion in the accounting and provide the accounting of disclosures to the Individual upon request.

Alternatively, Participant may refer the Individual to AHIE for access to One Health Record® if a protocol for Individual access is then currently available.

¹⁸ 45 CFR §164.528

AHIE Policy ## 013	Effective Date: October 1, 2023
Complaints	

Purpose

To ensure that there is a process by which Individuals may complain and/or make suggestions or other comments about practices or activities related to the AHIE, and/or its Participants and Authorized Users.

Policy

Complaint Management

The AHIE and all Participants shall accept complaints from Individuals about the practices or issues relating to the exchange of data between Participant and AHIE.

The AHIE will also accept complaints from Individuals, Participants, and Authorized Users specific to the AHIE's scope of service.

Any general complaint regarding the AHIE that is received by a Participant shall be forwarded to the Executive Director of the AHIE.

Complaints may be submitted in writing or by other reasonable method.

Neither the AHIE nor any Participant or Authorized User may retaliate, discriminate against, intimidate, coerce, or otherwise reprise an Individual if he or she files a complaint pursuant to this policy.

The foregoing complaint process does NOT limit nor change any rights that an Individual may have to file a complaint regarding any particular Healthcare Provider's privacy practices, in accordance with HIPAA.

Documentation of Complaints

Complaints submitted to the AHIE shall be documented in a Complaint Log.

Outcomes or resolutions to written complaints will be documented but may not be communicated to the submitting complainant unless specifically requested.

Nature of Complaints

Complaints submitted to the AHIE are not considered to be part of an Individual's record(s) shared by a Participant with AHIE.

Complaints submitted to the AHIE that include issues regarding the actions of an employee, agent or Business Associate of a Participant are subject to the following:

If a complaint includes information that may require action or response by a Participant or a member of the Participant's workforce or Business Associate, the complaint will be directed to the Participant to be addressed in accordance with Participant's internal practices and policies.

If a complaint includes information that may suggest violations of these AHIE policies, provisions of the Participation Agreement or other affirmative obligations of a Participant or Authorized User the complaint will be addressed by the Executive Director of the AHIE or his Designee.

AHIE Policy ## 014

Effective Date: October 1, 2023

Prohibition of Information Blocking**Purpose**

To support Participants' commitment to facilitate the timely access, exchange and use of electronic health information in compliance with applicable law.

Definition

Information Blocking refers to practices (i.e., acts or omissions) that are likely to prevent, materially discourage or otherwise interfere with the access, exchange or use of Electronic Health Information (EHI) including:

- The ability or means necessary to make EHI available for exchange or use (i.e., access to EHI),
- The ability for EHI to be transmitted between and among different technologies, systems, platforms, or network; and/or
- The ability for EHI, once accessed or exchanged, to be understood and acted upon (i.e., use of EHI).

Policy**Compliance with the Information Blocking Rule**

One Health Record® and its Participants will comply with all applicable federal and state law related to AHIE services, including the requirements of the Information Blocking Rule (if/when applicable).

Actors may be subject to penalties or disincentives if they violate the Information Blocking Rule by engaging in Information Blocking practices with the requisite level intent, and if the practice is not required by law or does not qualify as an exception.¹⁹ .

Neither the AHIE nor Participant Actors may engage in any practices that violate the Information Blocking Rule.

¹⁹ 45 CFR §§ 171.201 – 171.207

This policy does not prevent HIE or Participants from engaging in practices that are required by law or that fall within one of the exceptions listed in 45 CFR Subpart B.

AHIE and Participants are each independently responsible for identifying, assessing, and determining whether its own practices implicate the prohibition on Information Blocking, are required by law or qualify for an exception.

Information Blocking Complaint Management

Participants that reasonably believe AHIE or a Participant is violating the Information Blocking Rule in connection with the AHIE Services should promptly notify the Executive Director of AHIE.

AHIE may initiate an investigation into a complaint of Information Blocking involving a Participant and/or take other appropriate action, depending on the facts and circumstances surrounding the complaint.

Participants must cooperate with AHIE in any investigation into a complaint of Information Blocking, including providing upon reasonable request by AHIE an explanation of the practice alleged to constitute Information Blocking and/or producing any necessary or relevant documentation to support application of an exception.

Appendix A

Regulatory Foundation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, including, but not limited to:

- 45 CFR §160 General Administrative Requirements
- 45 CFR § 164 Subpart A General Provisions
- 45 CFR §164 Subpart C, Security Standards for the Protection of Electronic Protected Health Information (“The Security Rule”)
- 45 CFR §164 Subpart D Notification in the Case of Breach of Unsecured Protected Health Information (“The Breach Notification Rule”)
- 45 CFR §164 Subpart E Standards for Privacy of Individually Identifiable Health Information (“The Privacy Rule”)

The Health Information Technology for Economic and Clinical Health Act (HITECH)

- 42 USC §§17921-17953 enacted as part of the American Recovery and Reinvestment Act of 2009

The 21st Century Cures Act Final Rule 85 FR 25642, including:

- 45 CFR §170, Subpart B Office of National Coordinator Health Information Technology Standards
- 45 CFR § 170.213 Description of the United States Core Data for Interoperability (USCDI)
- 42 USC §300jj-52 “The Information Blocking Rule” and its implementing regulations at 45 CFR §171 Subparts A, B, and C

The Interoperability and Patient Access Final Rule 85 FR 25510 including additions of:

- 42 CFR § 431.60 Beneficiary access to and exchange of data, and
- 42 CFR § 457.730 Access to published provider directory information

Confidentiality of Substance Use Disorder Patient Records (Part 2)

- 42 CFR, Part 2, Subparts A, B, C, D, and E