Colorado Regional Health Information Organization (CORHIO)

Health Information Exchange
Governing Principles & Policies

Version 8.0

Approved by the CORHIO Board of Directors on

May 25, 2021

CORHIO Health Information Exchange Governing Principles & Policies Revision History		
Version	**Date**	**Notes**
8.0	May 25, 2021	Interim Review and Approval by the Policy Committee on April 27 and May 24: • Adopted No Information Blocking Policy; • Amended permitted uses to enable a Health Plan to query the Portal for Limited Healthcare Operations; • Updated Section 5.2.2 ("Use Purposes") to clarify CORHIO's obligations upon receipt of a subpoena or request from a government agency for Patient Information; • Clarified the Patient right of access Policy in Section 5.3 for consistency with No Information Blocking Policy and requirements; • Updated Section 8 to include new System Downtime, Maintenance, Update and Enhancement provision. Approved on 5/25/2021 by the CORHIO Board of Directors.
7.0	May 11, 2020	Interim Review and Approval by Policy Committee • Added new Section 5.2.8 to the Appropriate Use & Disclosure section expressly authorizing CORHIO to use and disclose PHI to public health authorities for permissible public health purposes. Approved on 5/11/2020 by CORHIO Board
6.6	June 5, 2019	Interim Review by Policy Committee • Added new HIE Participant to enable the onboarding of Correctional Institutions as defined in the HIPAA Privacy Rule. Approved on 7/23/2019 by CORHIO Board
6.5	June 29, 2018	Interim Review by Policy Committee • Support HIE participation for Coroners and Medical Examiners who are not in a HIPAA covered entity. Approved on 10/29/2018 by CORHIO Board
6.4	Jan. 27, 2017	Interim Review by Policy Committee • Added new HIE Participant to support patient- authorized exchange for life insurance determination and disability determination. Approved on 2/9/2017 by CORHIO Board
6.3	Jan. 15, 2016	Interim Review by Policy Committee • Added Section 5.4.1. Disclosure of Patient Information to a Personal Health Record to support CORHIO sending data to PHRs. Approved on 3/3/2016 by CORHIO Board
6.2	Sept. 11, 2015	Interim Review by Policy Committee • Establish policy to support participation by state-licensed health care providers who are not HIPAA covered entities. Approved on 9/30/2015 by CORHIO Board
6.1	March 13, 2015	Interim Review by Policy Committee • Clarify Policy regarding communications with other HIEs and healthcare entities. Approved on 4/1/2015 by CORHIO Board
6.0	April 24, 2014	Annual Review by Policy Committee • Major restructure to combine separate policy sections and eliminate redundancies.

		Approved on 5/27/2014 by CORHIO Board
5.1	Sept. 13, 2013	Interim Review by Policy Committee • Clarify Participant requirements regarding DURSA participation.
5.0	May 10, 2013	Annual Review by Policy Committee
4.1	Jan. 29, 2013	Interim Review by Policy Committee • Support CORHIO participation in nationwide health information exchange and the Data Use and Reciprocal Support Agreement (DURSA).
4.0	August 10, 2012	Annual Review by Policy Committee
3.1	Jan. 6, 2012	Interim Review by Policy Committee • Support HIE participation for clinical laboratories and health plans (payers).
3.0	July 21, 2011	Annual Review by Policy Committee
2.0	May 25, 2010	Operational review & updates
1.0	Nov. 29, 2007	Original Policies based on the Connecting for Health Common Framework created by the Markle Foundation.

Table of Contents

1. Governing Principles ---- *1*

1.1. Openness and Transparency ---- 1

1.2. Purpose Specification and Minimization ---- 1

1.3. Information Limitation ---- 1

1.4. Use Limitation ---- 1

1.5. Privacy Practices ---- 1

1.6. Information Integrity and Quality ---- 1

1.7. Security Safeguards and Controls ---- 1

1.8. Accountability and Oversight ---- 1

1.9. Security Breaches or Privacy Violations ---- 2

1.10. Compliance with Applicable Laws & Support for Emerging Standards and Practices ---- 2

2. Definitions ---- *3*

2.1. Construction ---- 3

2.2. Definitions ---- 3

3. Scope ---- *10*

4. Compliance with Law & Policies ---- *11*

4.1. Laws ---- 11

4.2. CORHIO Policies ---- 11

4.3. Participant Policies ---- 11

4.4. Compliance Management ---- 11

4.5. Communications with Other HIEs and Healthcare Organizations ---- 13

5. HIE Access and Use ---- *14*

5.1. User Authorization ---- 14

5.2. Appropriate Use & Disclosure ---- 15

5.3. Blocking Access to Suspect Patient Information ---- **Error! Bookmark not defined.**

5.4. Patient Participation and Access to the CORHIO System ---- 17

5.5. Auditing ---- 17

6. Privacy Practices ---- *18*

6.1. Patient Identification ---- 18

6.2. Informing Patients of CORHIO Participation ---- 19

6.3. Patient Participation and Choice Not to Use the CORHIO System ("Opt-Out") ---- 20

6.4. Patient Requests for Accounting of Disclosures ---- 20

6.5. Amendments to Patient Records ---- 21

7. Security Protocols ---- *22*

7.1. Secure Infrastructure ---- 22

7.2. Secure Patient Information ---- 22
7.3. End User Environment and Media Controls ---- 22
7.4. Participant Privacy and Security Policies & Procedures ---- 23
7.5. Data Integrity ---- 23
7.6. Risk Management ---- 23
7.7. Breach Mitigation ---- 23
7.8. Breach Notification ---- 24
7.9. Extended Policy: Review of Security Policies & Procedures for Participants That Are Not HIPAA Covered Entities ---- 24
8. Extended Policies: CORHIO & Its System Providers ---- *25*
8.1. Transparency & Accountability ---- 25
8.2. Security Considerations for Hardware/Software Development & Maintenance ---- 25
8.3. System Management ---- 25

1. Governing Principles

This section lists the governing principles that drive CORHIO's Health Information Exchange (HIE) development, operations, and other related activities.

1.1. Openness and Transparency

CORHIO supports a general policy of openness about developments, practices, and policies with respect to personal health information. Individuals and CORHIO participants should be able to know what personal health information exists, where it resides, the purposes for which it is used, and who can access and use it. Individuals should have safe, secure access to personal health information in a usable format and the ability to share that information with others involved in their care.

1.2. Purpose Specification and Minimization

The purposes for which personal health information is exchanged should be specified to individuals at the time information is initially collected. Subsequent use should be limited to those purposes, unless a change in purpose specification is provided to affected individuals.

1.3. Information Limitation

Personal health information should only be exchanged for specified purposes and should only be obtained by lawful and fair means, with the knowledge or consent of the affected individual, where possible.

1.4. Use Limitation

Personal health information should not be disclosed, made available, or otherwise used for purposes other than those specified.

1.5. Privacy Practices

Individuals have rights regarding personal health information about them. To support those rights:

- CORHIO will establish privacy practices to enable patient participation and will require its participants to do the same.
- Individuals should be able to obtain, from each entity that controls personal health information, verification of whether or not the entity has information relating to them.
- Individuals should be able to access and request amendments to their personal health information through CORHIO participant(s) from whom they receive their care, and participants should comply with their regulatory obligations in responding to such requests.
- CORHIO will not create or override any personal health information privacy or security rights or obligations.

1.6. Information Integrity and Quality

All personal health information provided to CORHIO should be accurate, current, and relevant to the purpose(s) for which it is to be used.

1.7. Security Safeguards and Controls

Personal health information should be protected by reasonable security measures, including administrative, physical, and technical safeguards, against such risks as loss, unauthorized access or modification, inadvertent destruction, or inappropriate use or disclosure.

1.8. Accountability and Oversight

Entities in control of personal health information, including CORHIO and its participants, must be held accountable for implementing these principles.

1.9. Security Breaches or Privacy Violations

CORHIO will develop and maintain processes to address any suspected security breaches or privacy violations.

1.10. Compliance with Applicable Laws & Support for Emerging Standards and Practices

CORHIO and its participants will comply with all applicable Laws regarding the protection of personal health information and will support emerging standards and best practices in the health information exchange field, to the extent technically feasible and practicable.

2. Definitions

2.1. Construction

Except where expressly stated otherwise, the following rules of interpretation apply to these CORHIO Policies: (i) "include," "includes," and "including" are not limiting and shall be deemed to be followed by "without limitation"; (ii) definitions contained in these Policies are applicable to the singular as well as the plural forms of such terms; (iii) the word "will" shall be construed to have the same meaning and effect as the word "shall" and vice versa; and (iv) the word "or" has, except where otherwise indicated, the inclusive meaning represented by the phrase "and/or."

2.2. Definitions

Defined terms are capitalized throughout these CORHIO Policies. If not defined in this section, such terms shall have the meaning assigned to them in the HIPAA Rules at 45 CFR Parts 160, 162, and 164.

2.2.1 HIE Participants

1. "Participant" means an individual or entity that (1) has entered into a written agreement with CORHIO to act as a Data Provider, Data Recipient, or both; and (2) falls into one (and only one) of the Participant Categories, as defined in the following table and may exchange Data through the HIE System for Permitted Purposes defined here and in the Participant Agreement:

Participant Category	HIPAA Role or Exception	Applicable HIE Policies	Available HIE Access Methods
Health Care Provider (HIPAA Covered Entity) • May be a public or private entity • As defined in the HIPAA Rules (see definition of "health care provider" at 45 CFR § 160.103)	• Covered Entity	• Standard Policies	• Data Query (incl. Portal) • EHR Interface • Data Feed

Health Care Provider (Not HIPAA Covered Entity)
• May be a public or private entity
• As defined in the HIPAA Rules (see definition of "health care provider" at 45 CFR § 160.103), but does not engage in HIPAA standard transactions and so is not a covered entity
• Must be a licensed health care professional, under state law.
	• Patient Authorization (As permitted by 45 CFR 164.508(a)(1)) obtained and maintained by health care provider prior to HIE access.	• Standard Policies
		• Extended Policies:
		  • Review of Security Policies & Procedures for Participants That Are Not HIPAA Covered Entities (Section 7.9)
		  • Add'l Required Audits for Participants That Are Not HIPAA Covered Entities (Section 5.5.6)
			• Data Query (incl. Portal)
			• EHR Interface
			• Data Feed

Health Plan (Payer) • May be a public or private entity • Must be a HIPAA Covered Entity As defined in the HIPAA Rules (see definition of "health plan" at 45 CFR § 160.103)	• Covered Entity	• Standard Policies	• Data Feed • Data Query (incl. Portal) for Limited Healthcare Operations purposes, provided Health Plan has or had an established relationship with the individual who is the subject of the Patient Information and the Patient Information pertains to that relationship

Provider or Payer Business Associate (BA) • Must be a BA of one or more current HIE Participants • Must have a HIPAA- compliant BA Agreement in place with one or more current Participant(s) • Applicable Participant(s) and CORHIO must agree to such access, in writing Such access may be utilized only in accordance with all Law and CORHIO Policies that apply to Participant(s)	• Business Associate	• Standard Policies	• Data Query (incl. Portal) • EHR Interface • Data Feed
Government Agency • Not a health care provider or health plan Not acting as a public health authority	• Patient Authorization (As permitted by 45 CFR 164.508(a)(1)) • CORHIO will refer any requests for Patient Information for judicial proceedings or law enforcement purposes, as permitted by 45 CFR 164.512(e) and 45 CFR 164.512(f), to the applicable Data Provider(s).	• Standard Policies • Extended Policy: • If Data Query (incl. Portal) access is provided, Add'l Required Audits for Participants That Are Not HIPAA Covered Entities (Section 5.5.6)	• Data Query (incl. Portal) • Data Feed

Organ Procurement Organization (OPO)
Must be a federally- sanctioned OPO
	• Uses and disclosures for cadaveric organ, eye or tissue donation purposes (As permitted by 45 CFR 164.512(h))	• Standard Policies
		• Extended Policies:
		  • Review of Security Policies & Procedures for Participants That Are Not HIPAA Covered Entities (Section 7.9)
		  • Add'l Required Audits for Participants That Are Not HIPAA Covered Entities (Section 5.5.6)
			• Data Query (incl. Portal)

Public Health Authority	• Uses and disclosures for public health activities • (As permitted by 45 CFR 164.512(b))	• Standard Policies	• Data Feed
Service Provider (Non- HIPAA Covered Entity) Requires access to patient information and HIPAA-compliant patient authorization to provide services, e.g., Life Insurance or Disability Insurance Provider	• Patient Authorization (As permitted by 45 CFR 164.508(a)(1)) obtained and maintained by participant prior to HIE access.	• Standard Policies • Extended Policies: • Review of Security Policies & Procedures for Participants That Are Not HIPAA Covered Entities (Section 7.9) • Add'l Required Audits for Participants That Are Not HIPAA Covered Entities	• Data Query

		(Section 5.5.6)	
Coroners and Medical Examiners (Non-HIPAA Covered Entity)	• Uses and disclosures for death evaluation purposes as permitted by 45 CFR 164.512(g)	• Standard Policies • Extended Policies: • Review of Security Policies & Procedures for Participants That Are Not HIPAA Covered Entities (Section 7.9) • Add'l Required Audits for Participants That Are Not HIPAA Covered Entities (Section 5.5.6)	• Data Query
Correctional Institution • As defined in the HIPAA Privacy Rule at 45 C.F.R § 164.501	• Uses and disclosures as permitted by 45 CFR 164.512(k)(5) and CRS § 27-70-101 et. seq.	• Standard Policies • Extended Policies: • Review of Security Policies & Procedures for Any Correctional Institutions That Are Not HIPAA Covered Entities (Section 7.9) • Add'l Required Audits for Participants That Are Not HIPAA Covered Entities (Section 5.5.6)	• Data Query (incl. Portal) • EHR Interface • Data Feed

2.2.2 Additional Definitions

1. Authorized Person / Point of Contact

"Authorized Person / Point of Contact" means an individual identified by a Participant to act as such Participant's point of contact to CORHIO for implementation and operational purposes.

2. Authorized User

"Authorized User" means the following:

- An individual approved and identified to CORHIO, by a Participant, to use the CORHIO System on behalf of such Participant, including a Workforce Member of the Participant or a medically-credentialed member of the Participant's medical staff;

- An individual who accesses Patient Information provided by the CORHIO System through a system-to-system level interface (the Participant is responsible for approving, identifying, and authenticating such Authorized Users); or

- A CORHIO Workforce Member whose role requires access to the CORHIO System.

3. Community Health Record

"Community Health Record" means a set of Patient Information regarding a particular individual that is combined from various sources throughout the Participant community over time (i.e., a "longitudinal" view) and made available through the CORHIO System.

4. CORHIO

"CORHIO" means the Colorado Regional Health Information Organization, including those individuals acting within the scope of their duties as Workforce Members of that organization.

5. CORHIO Policies

"CORHIO Policies" or "Policies" means these CORHIO Health Information Exchange Governing Principles & Policies and all CORHIO Procedures established thereunder.

6. CORHIO Policy Committee

"CORHIO Policy Committee" or "Committee" means the multi-stakeholder advisory committee established by CORHIO to provide advice and recommendations to CORHIO and the CORHIO Board of Directors regarding these CORHIO Policies. CORHIO Policy Committee members represent a variety of stakeholders, including various Participant types, government organizations, patient advocacy groups, and other interested parties.

7. CORHIO Procedures

"CORHIO Procedures" or "Procedures" means the rules, guidelines, and operational processes and procedures that CORHIO may, in its sole discretion, define and adopt to implement these CORHIO Policies or to otherwise maintain the privacy, security, confidentiality, integrity, and availability of the CORHIO System.

8. CORHIO System

"CORHIO System" means CORHIO's Internet-based authenticated system and search engine for patient health, demographic, and related information that facilitates the sharing and aggregation of Patient Information held by Participants with disparate health information systems, also known as "health information exchange (HIE)." The CORHIO System allows Authorized Users to communicate over a trusted network to access Patient Information. The CORHIO System may also support authenticated system-to-system level interfaces for those Participants who choose to provide their own end user interface components or for data transfer (i.e., Data Feed) purposes. The CORHIO System shall, at a minimum, conform to accepted nationwide standards for the interoperability of health information technology systems and health information exchange.

9. Credential

"Credential" means a user log-in/password combination or other technical means used by CORHIO to identify and authenticate an Authorized User for access to those CORHIO System components for which CORHIO provides an end user interface.

10. Data Feed

"Data Feed" means a method for Participants to access the CORHIO System such that CORHIO transfers a defined set of Patient Information to the Participant, according to an agreed upon technical specification.

11. Data Provider

"Data Provider" means a Participant that is authorized through its Participant Agreement, or other written agreement with CORHIO, to provide Patient Information to CORHIO for use through the CORHIO System.

12. Data Query

"Data Query" means a method for Participants to access the CORHIO System in which only applicable Patient Information is provided, according to the search criteria (i.e., "query") submitted. For example, Participants typically use a data query to access Patient Information in the Community Health Record.

13. Data Recipient

"Data Recipient" means a Participant that is authorized through its Participant Agreement, or other written agreement with CORHIO, to access the CORHIO System to obtain Patient Information.

14. Data Use and Reciprocal Support Agreement (DURSA)

"DURSA" means the legal, multi-party trust agreement that is entered into voluntarily by entities, organizations, and Federal agencies that desire to engage in electronic health information exchange with each other using an agreed upon set of national standards, services, and policies developed in coordination with the Office of the National Coordinator for Health IT (ONC) in the U.S. Department of Health and Human Services (HHS). Organizations that provide HIE services, like CORHIO, must join in the DURSA before they can participate in the public-private partnership maintained and operated eHealth Exchange, previously known as the "Nationwide Health Information Network (NwHIN)," and now referred to as "Healtheway™."

15. Direct Exchange

"Direct Exchange" means the transmission and receipt (i.e., exchange) of Patient Information between or among specific Participants where each such Participant has a relationship with the Patient about whom the information pertains. For example, a physician may receive lab results using Direct Exchange services provided by the CORHIO System.

16. EHR Interface

"EHR Interface" means a method for Participants to exchange Patient Information through the CORHIO System by means of direct technical integration between the Participant's electronic health record (EHR) system and the CORHIO System.

17. Extended Policy

"Extended Policy" means a portion of these CORHIO Policies that is only applicable to certain Participant Categories, or CORHIO and its System Providers, as specified.

18. HHS

"HHS" means the U.S. Department of Health and Human Services.

19. HIPAA

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations and rules promulgated thereunder, including the regulations found at 45 CFR Parts 160, 162, and 164 (the "HIPAA Rules").

20. HITECH

"HITECH" means the Health Information Technology for Economic and Clinical Health (HITECH) Act passed as a part of the American Recovery and Reinvestment Act (ARRA) of 2009 and the regulations and rules promulgated thereunder.

21. Lab Report

"Lab Report" means an electronic record of lab testing results that (1) is transmitted, stored, managed, or otherwise made available through the CORHIO System; and (2) complies with all applicable federal and state laboratory reporting laws and regulations, including the Clinical Laboratory Improvements Act of 1988 (CLIA), and the regulations promulgated thereunder.

22. Law

"Law" means any applicable statute, rule, regulation, legislation, constitution, common law, resolution, interpretation, ordinance, code, treaty, decree, directive, pronouncement, or other law of any federal, state, local, or other governmental authority.

23. Limited Healthcare Operations

"Limited Healthcare Operations" means the activities listed in paragraphs (1) and (2) of the definition Healthcare Operations at 45 C.F.R. §164.501, and Healthcare fraud and abuse detection and compliance activities as described at 45 C.F.R. § 164.506(c)(4).

24. NIST Special Publication (SP) 800-88

"NIST Special Publication (SP) 800-88" means the National Institute of Standards and Technology (NIST), Special Publication 800-88, Guidelines for Media Sanitization that describes how digital media (e.g., hard drives, disks, CDs, other media) should be handled or destroyed to protect sensitive information when it is no longer required, as called for by HHS guidance and the HIPAA Rules (available at http://csrc.nist.gov).

25. NIST Special Publication (SP) 800-111

"NIST Special Publication (SP) 800-111" means the National Institute of Standards and Technology (NIST), Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices that describes valid encryption processes for data at rest, as called for by HHS guidance and the HIPAA Rules (available at http://csrc.nist.gov).

26. Participant Agreement

"Participant Agreement" means the written agreement entered into by CORHIO and a Participant regarding the access, use, and sharing (i.e., "exchange") of Patient Information through the CORHIO System.

27. Patient

"Patient" means an individual who seeks treatment, care, coverage, or related services from a Participant or an individual about whom a Participant maintains personal health information. A Patient's rights may be exercised by the Patient or by a personal representative, as defined in the HIPAA Rules.

28. Patient Information

"Patient Information" means information regarding a specific individual provided by a Data Provider, pursuant to a Participant Agreement or other applicable agreement(s), including treatment and clinical information. Patient Information includes any personally identifiable information created, received, transmitted, stored, or otherwise managed by the CORHIO System and encompasses Protected Health Information (PHI).

29. Protected Health Information (PHI)

"Protected Health Information" or "PHI" has the meaning given to it under the HIPAA Rules, at 45 CFR §160.103, and shall include such information as is created, received, maintained, or transmitted by CORHIO or a Participant in connection with the CORHIO System.

30. Record

"Record" means a specific set of Patient Information accessed or assembled through the CORHIO System.

31. Standard Policies

"Standard Policies" means those portions of these CORHIO Policies that apply to all Participants and CORHIO and its System Providers. All portions of these CORHIO Policies are Standard Policies, unless otherwise stated.

32. System Interface

"System Interface" means any technical infrastructure that allows a Participant's system(s) to interact directly with the CORHIO System (in such cases, the Participant may choose to provide its own end user interface components).

33. System Provider

"System Provider" means any contractor, vendor, application service provider, hosting organization, managed services provider, or other individual or entity that supplies hardware, software, or services to CORHIO as support for any part of the CORHIO System.

34. Unsecured PHI

"Unsecured PHI" has the meaning given it by the HITECH Act, §13402(h), and includes Protected

Health Information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology as specified in the HIPAA Rules or by HHS guidance.

35. Workforce Member

"Workforce Member" means, as to CORHIO or a specific Participant or System Provider, an employee, contractor, subcontractor, agent, or other member of the workforce of that entity.

3. Scope

This section defines the scope and applicability of these CORHIO Policies.

These CORHIO Policies apply to the following groups, unless otherwise stated:

- Participants, including each Participant's Authorized Person(s)/Point(s) of Contact, its Authorized Users, and its Workforce Members;
- CORHIO and its Workforce Members; and
- CORHIO's System Providers, their Workforce Members, and others acting as agents or subcontractors on behalf of a System Provider regarding the CORHIO System.

Any reference to a "Participant" or "Participants" in these Policies includes the Participant's (or Participants') Authorized Person(s)/Point(s) of Contact, Authorized Users, and Workforce Members.

Any reference to "CORHIO" in these Policies includes CORHIO's Workforce Members. CORHIO requires that its System Providers adhere to these Policies. Accordingly, where these Policies apply to CORHIO, they shall be read as extending to such organizations. Certain components of these Policies may specifically refer to System Providers for emphasis, clarity, or to provide additional detail.

Some components of these CORHIO Policies apply only to certain Participant Categories or CORHIO and its System Providers. Such Extended Policies are demarcated by their section headings, and the groups to which they apply are specifically stated. All other portions of these CORHIO Policies are Standard Policies that apply to all Participants and CORHIO and its System Providers.

In furtherance of these CORHIO Policies, CORHIO may, in its sole discretion, define and distribute additional detailed processes or procedures (the "CORHIO Procedures") to maintain the privacy, security, confidentiality, integrity, and availability of the CORHIO System.

4. Compliance with Law & Policies

This section sets compliance expectations, describes policy requirements for Participants, and explains CORHIO's approach to compliance management. Compliance expectations regarding CORHIO's DURSA participation, and interaction with other healthcare entities, outside the DURSA community, in support of community, regional, interstate and nationwide health information exchange, are also detailed.

4.1. Laws

CORHIO and Participants shall, at all times, comply with all Laws, including those that protect the privacy and security of Patient Information and establish certain individual privacy rights (e.g., HIPAA, HITECH). CORHIO and Participants shall use reasonable efforts to stay abreast of any updates to or changes in interpretations of such Laws and shall each designate a privacy official and a security official to ensure compliance.

4.2. CORHIO Policies

CORHIO and Participants shall, at all times, comply with all applicable CORHIO Policies. These CORHIO Policies may be revised and updated from time to time, and such revisions and updates shall be effective upon notice to Participants, as specified in the Participant Agreement(s) and any other applicable agreements. Participants are responsible for ensuring they have, and are in compliance with, the most recent version of these CORHIO Policies.

4.2.1 Policy Review

1. These CORHIO Policies shall be reviewed from time to time, but not less often than annually, by CORHIO and the CORHIO Policy Committee. The Committee shall submit any proposed revisions to the CORHIO Board of Directors for review and approval.

2. The CORHIO System will support generally-accepted industry standard data formats, messaging protocols, and other accepted technology and operational standards, including those required under the DURSA, those that may be needed to support interaction with other healthcare entities, outside the DURSA community, and those required by Law. As a part of the policy review process, CORHIO will periodically perform a survey and analysis of generally-accepted industry standards and Laws that may impact these CORHIO Policies.

4.3. Participant Policies

Participants are responsible for ensuring that they have the requisite, appropriate, and necessary internal policies to comply with applicable Laws and these CORHIO Policies. Participants may choose to adopt and implement policies that are more protective of the privacy and security of Patient Information than these CORHIO Policies.

Participants may not make agreements with any parties that may impair CORHIO's ability to comply with applicable Laws or generally-accepted certification or accreditation criteria applicable to CORHIO or its System Providers.

Participants shall refer to and comply with their own internal policies and procedures regarding Patient Information uses and disclosures, the conditions that must be met, and any documentation that must be obtained prior to such uses or disclosures.

4.4. Compliance Management

A Participant Agreement, or other applicable agreement, that requires adherence to these CORHIO Policies must be executed between CORHIO and a Participant prior to such Participant accessing or exchanging Patient Information through the CORHIO System.

To ensure compliance with these CORHIO Policies, CORHIO may, on a periodic basis, require Participants to provide information regarding or access to Participant policies, procedures, Authorized Person(s)/Point(s) of Contact, Authorized Users, or work environments for audit or review purposes.

CORHIO will maintain copies of these CORHIO Policies (and previous versions) for a minimum of six (6) years or for such longer period as may be required by Law.

4.4.1 Participant Authorized Person/Point of Contact

Participants must designate at least one Authorized Person/Point of Contact, who must be recognized by CORHIO prior to making any requests. Participants are strongly encouraged to designate an additional Authorized Person, in case the primary Point of Contact is unavailable. The Authorized Person may request Credentials and access auditing reports, as appropriate. Such individual also acts as an administrative point of contact to CORHIO on the Participant's behalf and is responsible for ensuring compliance with any applicable agreements, such as the Participant Agreement, and these CORHIO Policies. The Point of Contact shall be prepared to interact with CORHIO and help coordinate risk mitigation and security event (e.g., data breach, unauthorized use investigation) activities.

4.4.2 Training and Acknowledgement

1. CORHIO shall develop and distribute training and educational materials to support Participants' implementation and appropriate use of the CORHIO System. Participants shall implement a training process for their Workforce Members who will have access to the CORHIO System to ensure compliance with these CORHIO Policies. Such training shall include a detailed review of applicable CORHIO Policies.

2. CORHIO will provide Participants with an agreement that must be signed by all Authorized Users ("Authorized User Agreement") at the completion of such training attesting that they each have received, read, understand, and will comply with these CORHIO Policies. Alternatively, a Participant may add CORHIO-approved content to its existing user agreement(s) and amend its current processes as necessary and approved by CORHIO.

3. Participants shall maintain documentation regarding their training and acknowledgement process in accordance with these CORHIO Policies and applicable

4. Laws. For audit or review purposes, CORHIO may, from time to time, require that Participants provide information regarding, or access to, such documentation.

5. CORHIO shall institute a training process for its Workforce Members to ensure compliance with these CORHIO Policies. The training shall include a detailed review of applicable CORHIO Policies and each trained Workforce Member shall sign a representation that he or she has received, read, understands, and will comply with these CORHIO Policies. This training shall occur within a reasonable time for new hires and at least annually for all CORHIO Workforce Members. CORHIO shall maintain documentation regarding its training and acknowledgement process in accordance with applicable Laws.

4.4.3 Reporting Non-Compliance

1. Participants shall have a mechanism for its Workforce Members to report any non- compliance with these CORHIO Policies and shall encourage them to do so. Participants shall establish a process for individuals whose Patient Information is accessible through the CORHIO System to report any non-compliance with applicable Laws or these CORHIO Policies or any other concerns about improper disclosures of Patient Information.

2. CORHIO shall establish a process for individuals whose Patient Information is accessible through the CORHIO System, Participants, and others to report any non- compliance with these CORHIO Policies or applicable Laws or concerns about improper disclosures of Patient Information. CORHIO shall also establish a process for individuals and Participants to notify CORHIO regarding any potential inappropriate or unauthorized use of the CORHIO System.

4.4.4 Sanctions for Non-Compliance

1. Participants who fail to comply with these CORHIO Policies shall be subject to review by CORHIO and may have access to the CORHIO System terminated.

2. Considering the highly sensitive nature of Patient Information, CORHIO maintains a zero-tolerance policy regarding inappropriate or unauthorized use of the CORHIO System. Authorized Users who violate these CORHIO Policies, as identified through reporting, auditing, or other processes, may be sanctioned as defined in the CORHIO Procedures, and the applicable Participant shall be notified so that disciplinary action in accordance with the Participant's own internal policies can be pursued.

3. Participants shall implement procedures to discipline and hold Workforce Members accountable for complying with these CORHIO Policies and ensuring that they do not access, use, disclose, or request Patient Information except as permitted by these CORHIO Policies. If non-compliance occurs, CORHIO shall be notified and the individual's access may be terminated, according to the sanctions defined in the CORHIO Procedures. Participants may choose to take additional actions according to their own sanctioning policies.

4. All CORHIO Workforce Members shall be accountable for ensuring that they comply with these CORHIO Policies and do not use, disclose, or request Patient Information except as permitted by these CORHIO Policies. In the event that non-compliance is detected or reported, disciplinary measures shall include, but may not be limited to, verbal and written warnings, demotion, loss of Authorized User status, termination of employment, or retraining as appropriate.

4.5. Communications with Other HIEs and Healthcare Organizations

CORHIO may enter into agreements that enable health information exchange across different states, regions, communities, and with other healthcare organizations. Such agreements may expand CORHIO's reach and provide data exchanges with the participants of other HIEs. CORHIO shall be responsible for confirming that the policies of such other HIEs and healthcare organizations are at least as protective of Patient Information as specified in these CORHIO Policies, its Participant Agreement(s), and any other applicable agreements (and may do so by requiring that such other HIEs and healthcare organizations agree to join and comply with the terms of the DURSA, as described below).

4.5.1 Participation in the Data Use and Reciprocal Support Agreement (DURSA)

1. CORHIO may become a party to the Data Use and Reciprocal Support Agreement (DURSA). The DURSA is a legal, multi-party trust agreement that is entered into voluntarily by all entities, organizations, and Federal agencies that desire to engage in electronic health information exchange with each other using an agreed upon set of national standards, services, and policies developed in coordination with the Office of the National Coordinator for Health IT (ONC) in the U.S. Department of Health and Human Services (HHS). Organizations that provide HIE services, like CORHIO, and other healthcare organizations must first join in the DURSA before they can participate in the eHealth Exchange, a public-private partnership for national health information exchange previously known as the "Nationwide Health Information Network (NwHIN)," and now referred to as "Healtheway™." Note that as described in Section 4.5 above, CORHIO may enter into agreements with other HIEs and healthcare organizations to support health information exchange, in addition to the DURSA.

2. The DURSA is in alignment with these CORHIO Policies and reaffirms the obligations of CORHIO and its Participants to comply with applicable Laws (e.g., HIPAA, state and federal privacy and security statutes and regulations). CORHIO Participants must recognize that they are part of this broader HIE community as a result of CORHIO's participation in the DURSA and the eHealth Exchange. To that end, CORHIO Participants must adhere to the applicable terms of the DURSA and any applicable operating policies and procedures of the eHealth Exchange, all of which are publicly available, including those governing the use, confidentiality, privacy, and security of Patient Information exchanged through the eHealth Exchange.

3. CORHIO Participants must (1) reasonably cooperate with CORHIO on issues related to the DURSA; (2) exchange Patient Information through the eHealth Exchange only for a "permitted purpose" as defined by these CORHIO Policies and the DURSA; (3) use Patient Information received through the eHealth Exchange only in accordance with the terms of the DURSA; and (4) notify CORHIO as soon as reasonably practicable after determining that a data breach has occurred, so that CORHIO may comply with the breach notification terms of the DURSA and eHealth Exchange operating policies and procedures.

4. Recognizing that the terms of the DURSA and eHealth Exchange operating policies and procedures are subject to change, CORHIO will implement and maintain procedures to provide Participants with information regarding the DURSA and eHealth Exchange operating policies and procedures, including any opportunities to comment on, object to, or approve of changes to those requirements.

5. HIE Access and Use

This section defines how access to the CORHIO System is established. Appropriate uses and disclosures of Patient Information are also defined, and policies regarding Patient access and auditing processes are detailed.

5.1. User Authorization

Access to the CORHIO System and Patient Information is limited to Authorized Users.

5.1.1 Secure Access, Authorization, and Authentication

1. CORHIO shall only facilitate access to Patient Information for Authorized Users. Participants shall follow, at a minimum, any identification or authentication requirements as required by applicable Laws or CORHIO Policies or Procedures to verify the identity of those Workforce Members who shall be deemed to be Authorized Users and granted access to Patient Information through the CORHIO System.

2. CORHIO shall provide Participants with Credentials for Authorized Users who utilize CORHIO-supplied end user interface components. CORHIO shall maintain a master list of all Authorized Users for whom such Credentials have been established and will use reasonable efforts to maintain the current status of such Authorized Users (See Section 5.1.3, Changes to Authorized Users). CORHIO shall establish terms and conditions for log-in using CORHIO-supplied Credentials. Detailed rules regarding strong passwords, access suspension, password expiration, password caching, and automatic log off shall be provided in the CORHIO Procedures and are subject to change, as needed, to meet current industry standards and as required by Law.

3. In addition to user level authentication, where applicable, the CORHIO System will also authenticate the requesting organization using agreed upon technical standards at the time a request is made. To the extent technically feasible, CORHIO shall support federated user authentication through the use of cross-enterprise secure transactions that contain sufficient identity information to make reasonable access control decisions and produce appropriate audit logs.

5.1.2 Authorized User Identification

CORHIO and Participants shall allow access to the CORHIO System only by those Workforce Members who have a legitimate and appropriate need to use the CORHIO System or release or obtain Patient Information through the CORHIO System. No Workforce Member shall be provided with access to the CORHIO System or Patient Information obtained from it without first having been trained on these CORHIO Policies, to the extent applicable (See Section 4.4.2, Training and Acknowledgement).

Each Participant's Point of Contact shall identify those to be treated as Authorized Users by CORHIO, coordinate Authorized User training, and maintain Authorized User information and status. Authorized Users are responsible for all actions performed under their Credentials. Authorized Users may only utilize the CORHIO System for appropriate uses under these CORHIO Policies (See Section 5.2,

Appropriate Use & Disclosure).

5.1.3 Changes to Authorized Users

Participants shall be responsible for notifying CORHIO when there is a change to their Authorized Users who have been granted Credentials by CORHIO, including any current Authorized Users who no longer have a legitimate need to access the CORHIO System as a part of their duties.

5.1.3.1 Change Includes Authorized User Disciplinary Action

If a change relates to an Authorized User who has been disciplined for using, disclosing, or requesting Patient Information in a manner not permitted by these CORHIO Policies or non-compliance with applicable Laws or these CORHIO Policies, the notification shall occur immediately, and under no circumstances, in more than 24 hours. This notification may be followed by sanctions against the non-compliant individual or Participant, as defined in the CORHIO Procedures.

5.1.3.2 Change Does Not Include Authorized User Disciplinary Action

If a change is unrelated to non-compliance with applicable Laws or these CORHIO Policies, the notification shall be made to update the Authorized User status as soon as possible, within a maximum of 72 hours.

5.1.4 No Log-In/Password Sharing

CORHIO assigns unique Credentials to Authorized Users and maintains a zero- tolerance policy towards log-in/password sharing. Participants must ensure that all Authorized Users understand that (1) Credentials are not to be shared; and (2) any violation of this policy may be deemed inappropriate use and result in sanctions as defined in the CORHIO Procedures.

5.2. Appropriate Use & Disclosure

Patient Information available through the CORHIO System may only be used and disclosed in a manner that is consistent with applicable Laws and these CORHIO Policies. Data Providers are responsible for ensuring proper Patient authorization, if required by Law, is obtained prior to sharing Patient Information for use and disclosure through the CORHIO System. Any Patient Information supplied by a Data Provider will be deemed to be authorized for sharing through the CORHIO System unless the Data Provider supplies an indicator that the Patient has opted out of sharing (See Section 6.3, Patient Participation and Choice Not to Use the CORHIO System ("Opt-Out")).

5.2.1 Appropriate Use

1. CORHIO shall provide Participants with supporting information, rules, and standards for use of the CORHIO System. Participants shall establish and maintain internal policies and procedures that effectively manage access to, and the appropriate use of, Patient Information in the CORHIO System.

5.2.2 Use Purposes

1. Participants shall provide or request Patient Information through the CORHIO System only for purposes permitted by Law, the Participant Agreement and these CORHIO Policies. Patient Information may only be requested and shared through the CORHIO System by and between parties that have agreed to such sharing and in a manner that is consistent with all applicable Laws.

2. Participants shall only request Patient Information through the CORHIO System for permissible purposes as defined by Law. In the absence of a permissible purpose, Participants shall not access Patient Information through the CORHIO System. Regardless of whether permitted by Law, the following uses of Patient Information are prohibited:

- Any Marketing purposes;

- Any Fundraising purposes;
- Any Health Insurance Underwriting purposes; and
- Any decisions related to health insurance enrollment and eligibility (e.g., issuing, denying, cancelling coverage), except as permitted pursuant to an agreement executed between CORHIO and a Government Agency Participant.

3. If CORHIO or any of its subcontractors or third party vendors receives a court order or subpoena for Patient Information, or a request for Patient Information by a government entity pursuant to applicable Law, CORHIO, to the extent permitted by applicable Law, will provide timely notice to the Participant that provided the Patient Information, if known, as soon as possible after receipt of the request, so that the Participant has an opportunity to object to the court order, subpoena or governmental request (in accordance with the stated timelines in the request). CORHIO will not be responsible for contesting or objecting to any such court order, subpoena or governmental request, but will reasonably assist a Participant in its efforts to do so at no cost to CORHIO. CORHIO will comply with applicable Law, including Colo. R. Civ. Proc. 45, in responding to subpoenas.

5.2.3 Use & Disclosure of Laboratory Test Results

By participating in the HIE, as provided through the CORHIO System, Participants who are health care providers authorize CORHIO to access Lab Reports directly from clinical laboratories on their behalf and provide such Lab Reports through the CORHIO System.

5.2.4 No Discrimination

CORHIO does not permit the use of Patient Information for unlawful discriminatory purposes. Under no circumstances shall Patient Information be accessed or disclosed for an unlawful discriminatory purpose. If and when CORHIO should become aware that Patient Information has been accessed, disclosed, or otherwise utilized for an unlawful discriminatory purpose, the responsible Participant(s) or Authorized User(s) may be subject to sanctions for inappropriate use as defined in the CORHIO Procedures.

5.2.5 Incorrect or Inappropriate Use or Disclosure

In the event that Patient Information is used or disclosed for other than permissible purposes, CORHIO and the Participant(s) involved with or affected by any such use or disclosure will work together to investigate and resolve the incident according to these CORHIO Policies (See Sections 7.7-7.8, Breach Mitigation and Breach Notification).

5.2.6 Re-disclosure Prohibition

Participants may not re-disclose Patient Information accessed through the CORHIO System to other persons except for the purposes for which the Patient Information was accessed, as required by Law, or as otherwise expressly permitted by the Participant Agreement, or other applicable Agreement(s). This also prohibits re-disclosure to a Patient's employer, except as authorized by Law.

5.2.7 Patient Information Subject to Special Protection

Federal and state laws impose heightened privacy and security requirements upon the disclosure of certain types of Patient Information that may be considered particularly private or sensitive (e.g., alcohol and substance abuse treatment records, psychotherapy notes, services paid for out-of-pocket when requested). Any disclosure of Patient Information must be conducted in compliance with all applicable Laws. Data Providers are responsible for complying with such Laws and shall determine what (if any) Patient Information is subject to special protection prior to making it available through the CORHIO System.

5.2.8 Use and Disclosure for Permissible Public Health Activities.

Except as otherwise limited by applicable Laws, Policies or CORHIO's contractual obligations, CORHIO may disclose PHI without Patient authorization to a public health authority who is legally authorized to receive and use such information for permissible public health purposes, including by way of example and not limitation, for the reporting of a disease or injury; reporting vital events, immunization information, or cancer cases; and conducting public health surveillance, investigations, or interventions. CORHIO will limit PHI disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. However, CORHIO may reasonably rely on a minimum necessary determination made by the public health authority in requesting the PHI.

5.3. Patient Participation and Access to the CORHIO System

Federal laws, including HIPAA, give individuals the right to access their health information, unless an exception to the individual right of access applies. Because CORHIO does not have a direct relationship with individuals whose Data is accessible through the HIE, CORHIO relies on Participants to manage relationships and disclosures of Patient Information from the CORHIO System to Patients. Patients who contact CORHIO regarding their Patient Information shall be referred to one or more of the Participants where they receive care. Due to legal, technical, and administrative limitations, the CORHIO System does not currently support alternative means by which Patients may access their Data through the HIE, such as through an individual access portal or other automated means. CORHIO may pilot or develop projects to facilitate Patient access to Patient Information available through the CORHIO System, but such functions will require approval, involvement, and/or action on the part of interested Participants.

5.3.1 Disclosure of Patient Information to a Personal Health Record

A Participant may use the CORHIO HIE to disclose Patient Information to a Personal Health Record ("PHR") vendor that is a Business Associate of the Participant, provided

- (i) a HIPAA-compliant BA Agreement between PHR Vendor and Participant is in place,
- (ii) CORHIO and the Participant to which a PHR Vendor serves as a BA agree to allow such access in writing, and
- (iii) such access may be utilized only in accordance with all Law and CORHIO Policies. In such a scenario, no Patient would have access to the HIE or the CORHIO System.

5.4. Auditing

CORHIO will audit use of the CORHIO System to ensure system accuracy and compliance with Participant Agreements, other applicable agreements, and these CORHIO Policies. In addition, security administration functions, system administration functions, and other system-level activities will be logged and monitored in system management logs (See Section 8.3.5, System Maintenance and Operations).

5.4.1 Audit Log

CORHIO shall establish and maintain an audit log that documents all log-in events and which Authorized Users, Data Providers, or System Interfaces post, modify, access, or otherwise interact with Patient Information in the CORHIO System, including details regarding the action(s) taken. The CORHIO System shall have the ability to log Authorized User actions that, at a minimum, meets the requirements specified by applicable Laws, including the HIPAA Rules (log content details are documented in the CORHIO Procedures).

CORHIO will make audit log information available to Participant Authorized Persons/Points of Contact upon request for purposes such as responding to Patient requests, managing compliance, and conducting investigations. Appropriately formatted Authorized User activity and Patient Information disclosure logs will be available to Participant Authorized Persons/Points of Contact on demand, with direct access available to the extent reasonable and technically feasible.

5.4.2 Audit Log Controls

Audit logs shall be protected against unauthorized access, modifications, and deletion.

5.4.3 Audit Log Availability & Retention

Audit logs shall be readily available for six (6) months and archived in accordance with applicable Laws, for a minimum of six (6) years past the current year.

5.4.4 System Audits

CORHIO shall conduct periodic audits to ensure the adequacy of the Master Patient Index (MPI) and its patient matching algorithms.

CORHIO may periodically activate, facilitate, or conduct system audits to review Authorized User or system activities, as defined in the CORHIO Procedures. Participant Authorized Persons/Points of Contact may request audits of specific Authorized Users or activities.

5.4.5 Participant and Authorized User Audits

Random audits of Participants and Authorized Users may be conducted periodically. Random audits will focus on records held by the CORHIO System and shall be conducted by CORHIO or a CORHIO-authorized independent third-party. CORHIO shall notify the relevant Participant(s) of any inappropriate use, privacy, or security breach identified through such audits.

5.4.6 Extended Policy: Add'l Required Audits for Participants That Are Not HIPAA Covered Entities

Participants that are not HIPAA Covered Entities are subject to additional auditing and organization-level reporting requirements regarding Authorized User activities. Periodically, CORHIO will provide the Authorized Persons/Points of Contact for such Participants with reports detailing Authorized User activities. Participants must review and validate all Authorized User activities described in such reports to ensure that all applicable conditions or requirements for Patient Information use and disclosure have been met. Further details regarding audit protocols, including required Participant feedback, are documented in the CORHIO Procedures.

6. Privacy Practices

This section establishes requirements for CORHIO and Participant privacy practices, including standards for Patient identification and participation.

6.1. Patient Identification

For query purposes, the CORHIO System shall require that a minimum set of data be provided to identify and match records for a particular Patient. This minimum data set shall be designed to minimize, to the extent possible, any incidental uses or disclosures of Patient Information.

6.1.1 Master Patient Index

CORHIO shall establish a Master Patient Index (MPI) of specific demographic data to facilitate access to Patient Information. CORHIO shall store and maintain the demographic information submitted by each Participant and create a systematic link between records. CORHIO shall protect the Patient Information stored in the MPI in accordance with applicable Laws and these CORHIO Policies.

6.1.1.1 Computer-Based Matching System

CORHIO shall use a computer-based configurable algorithm to assist in linking records in the MPI that pertain to the same Patient when receiving Patient Records from Participants.

6.1.1.2 Patient Identification Data Integrity Process

CORHIO will build, maintain, and, as appropriate, share with Participants reports to review ambiguous or potentially duplicate records submitted by Participants. When CORHIO provides feedback to a specific Participant, that Participant is expected to research the situation(s) in a

timely manner and respond with the results of its internal analysis. Participants agree to act on such analyses and conduct quality improvement efforts to minimize subsequent ambiguous or potentially duplicate data submissions (i.e., to limit perpetuating ambiguous information).

6.1.1.3 Usage Limitation on Social Security Number and Government-Approved Identification Numbers

Subject to applicable Laws, CORHIO shall design its computer-based matching system to limit the use of Social Security Numbers, or other government-approved identification numbers, in a manner that balances Patient privacy with the need to match Patients accurately (See the CORHIO Procedures for implementation details).

6.1.2 Patient Query

An Authorized User shall query the MPI and view Patient demographic information only in accordance with these CORHIO Policies. When searching the MPI, Authorized Users must provide, at a minimum, the mandatory data fields, as required by the CORHIO Procedures. If the Participant does not have an established clinical relationship with the Patient, the Authorized User may be required to take additional actions to access Patient Information, as described in the CORHIO Procedures. Participants that are not health care providers shall only be given access to Patient Information that has been specifically authorized by agreement with CORHIO. Health Plan Participants may only access Patient Information pertaining to individuals with whom they have a current relationship, as defined by their Participant Agreements, other applicable agreement(s), and applicable Laws.

6.1.3 Action Required for Incorrect Match

Participants shall report search results that indicate an incorrect Patient match has occurred to CORHIO on an as soon as possible basis. CORHIO will review these instances, conduct an audit, and initiate a process to de-link the affected records, as appropriate.

6.1.4 Action Required for Non-Matching Clinical Disclosures

If an Authorized User recognizes that Patient Information received from CORHIO does not apply to the Patient about whom information was requested, the Authorized User shall take reasonable steps to immediately destroy that Patient Information, including, where applicable, deleting the Patient Information received from CORHIO and properly disposing of any paper or electronic copies. The Authorized User shall contact CORHIO, or the appropriate Authorized Person / Point of Contact who shall alert CORHIO to the occurrence. CORHIO will maintain records, including audit logs, as required by these CORHIO Policies and Law, and will follow its breach response procedures, as appropriate.

6.2. Informing Patients of CORHIO Participation

Participants shall maintain a Patient notification process (or, as applicable, a patient authorization process) that complies with applicable Laws, including the HIPAA Rules. Participants are responsible for their own compliance with the HIPAA Rules and other applicable Laws. CORHIO will provide Participants with a sample Patient notification document that complies with these CORHIO Policies. Participants shall have the option to either use the CORHIO-provided sample or incorporate the information provided by CORHIO into their own Patient notification process (the "CORHIO Notice").

Participants shall have their own policies and procedures governing distribution of the CORHIO Notice to Patients, which shall comply with these CORHIO Policies and all applicable Laws, including the HIPAA Rules.

6.2.1 Notice Content

The CORHIO Notice shall meet the content requirements set forth under the HIPAA Rules and otherwise comply with all applicable Laws. The CORHIO Notice also shall include a description of the CORHIO System and inform Patients regarding: (1) what information the Participant may include in and

make available through the CORHIO System; (2) who is able to access the information through the CORHIO System; (3) for what purposes such information can be accessed; and (4) how a Patient may choose to not have his or her information shared through the CORHIO System.

6.3. Patient Participation and Choice Not to Use the CORHIO System ("Opt-Out")

Demographic information for all Patients served by Participants shall be included in the MPI for matching purposes. Patients may choose to not allow Patient Information to be shared through the CORHIO Community Health Record ("opt-out"). When a query is made for such a Patient's information in the Community Health Record, only demographic information shall be displayed with an indicator that the Patient has opted- out of information sharing. Any additional actions taken by an Authorized User to search or create new Patient Records in the Community Health Record, after receiving the indicator that the Patient has opted-out of information sharing, may be deemed an inappropriate use of the CORHIO System and subject to sanctions.

6.3.1 Patient Choice Processes

1. Participants and CORHIO shall establish reasonable and appropriate processes, at the Participant point of care, to enable the exercise of a Patient's choice not to have information about him or her shared through the CORHIO System. Participants retain the responsibility for determining the specific process by which patients may exercise their choice.

2. CORHIO shall also establish and maintain a secondary process to allow Patients to choose not to have Patient Information made available through the CORHIO System, other than for Direct Exchange between Participants with whom the Patient has an established relationship. CORHIO shall make the secondary process accessible to the general public.

6.3.2 Effect of Choice

A Patient's choice to not allow information sharing through the CORHIO System may be exercised through the Participant, as described in the Participant's CORHIO Notice or through a secondary process supported by CORHIO. A Patient's choice to not share information through the CORHIO System shall apply to information sharing through the Community Health Record, sometimes called "query" or "indirect exchange." Simple results delivery to Participants with which the Patient has an established relationship (e.g., lab results), or exchanges of Patient Information among Participants with which the Patient has an established relationship, also known as Direct Exchange, may still take place through the CORHIO System.

6.3.3 Opt-Out Revocation

A Patient who has chosen to opt-out of information sharing through the CORHIO System may subsequently choose to allow sharing of his or her Patient Information going forward, by revoking his or her decision through a Participant's notification and authorization process. A Patient may also revoke his or her prior decision to opt-out by utilizing the secondary process provided by CORHIO.

6.3.4 Patient Choice Documentation

CORHIO and Participants shall document and maintain such documentation of all Patients' decisions not to have Patient Information shared through the CORHIO System and any revocations of such decisions, for a minimum of six (6) years and in accordance with all applicable Laws. Participants shall inform CORHIO of Patients' choices according to methods established in the CORHIO Procedures. For audit or review purposes, CORHIO may, from time to time, require Participants to provide information regarding or access to such documentation.

6.4. Patient Requests for Accounting of Disclosures

Participants shall have policies and procedures to respond to Patient requests for accounting of disclosures, in keeping with applicable Laws, including the HIPAA Rules. Participants will have access to information regarding

all Patient Information uses and disclosures through the CORHIO System, allowing Patients to obtain all disclosure accounting related to the CORHIO System from a single Participant, to the extent technically feasible. If contacted by Patients, CORHIO shall direct them to contact one or more of the Participants where they receive care.

6.5. Amendments to Patient Records

CORHIO shall not make changes to Patient Records. Patients must request amendments through the Participant(s), according to processes established and managed by the Participant(s).

If a Participant amends a record, it may access or, if necessary, request an accounting of disclosures from CORHIO for the purpose of notifying other Participants as may be required to comply with the HIPAA Rules.

7. Security Protocols

This section defines security protocols that must be utilized by CORHIO, its System Providers, and Participants to protect the confidentiality, integrity, and availability of the Patient Information that is created, received, transmitted, stored, or otherwise managed by the CORHIO System.

CORHIO, its System Providers, and Participants shall establish an appropriate and generally-accepted level of security controls, including administrative, physical, and technical safeguards, by employing industry standard security technologies and processes. At a minimum, such safeguards shall reasonably and appropriately protect the confidentiality, integrity, and availability of Patient Information as required by applicable Laws, including the HIPAA Rules.

7.1. Secure Infrastructure

CORHIO, its System Providers, and Participants shall only allow Authorized Users and CORHIO System operations personnel to access the CORHIO System from secured end user environments.

CORHIO shall provide technical security specifications to Participants as part of the implementation process. As a condition of implementation and to support ongoing risk assessment, CORHIO may request a network component diagram and standard document from Participants to ensure that appropriate hardware and software has been implemented and is maintained on an ongoing basis.

In accordance with the Participant Agreement, or other applicable agreement(s), CORHIO will assist new and established Participants regarding expected security standards. CORHIO may assess Participant conformance using test and production environments, and Participants must demonstrate compliance with CORHIO security protocols prior to use of the CORHIO System.

CORHIO will implement and maintain appropriate technical safeguards for the CORHIO System, including hardware and software protective mechanisms such as firewalls, intrusion detection and prevention, anti-virus, and protected networks (e.g., network infrastructure, remote access, and wireless networking controls). Internal CORHIO System databases shall not be accessible from any external website or the Internet, except by Authorized Users or authorized CORHIO System operations personnel using secured interfaces. Potential intrusion or other security incidents shall be tracked as part of CORHIO's breach response, risk management, and audit processes, as appropriate.

Participants shall conform to CORHIO's requirements for secure infrastructure and data transmission including appropriate hardware and software protective mechanisms such as firewalls, anti-virus, intrusion detection and prevention, and protected networks (e.g., network infrastructure, remote access, and wireless networking controls).

7.2. Secure Patient Information

Patient Information or the transmission of Patient Information submitted to, managed, or delivered by the CORHIO System shall be encrypted and secured, to the extent reasonable and technically feasible, according to technical specifications approved by CORHIO that, at a minimum, satisfy the HHS guidance provided under HITECH §13402(h) regarding Unsecured PHI and minimize the impact of any data breach.

7.3. End User Environment and Media Controls

CORHIO, its System Providers, and Participants shall employ reasonable security controls for all personal computers, laptops, or workstations used to access the CORHIO System, including implementing anti-virus protection, updating systems to mitigate known vulnerabilities (i.e., "patching"), providing a session timeout to prevent inadvertent access to end user interface components supplied by the CORHIO System, and minimizing the use of Internet services that may risk the introduction of spyware or other malicious software, to the extent feasible.

CORHIO, its System Providers, and Participants shall ensure that any Patient Information stored on portable or mobile devices is protected by adequate security controls (e.g., access controls, remote wiping, encryption per

NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices) and that all media containing Patient Information is rendered unreadable prior to disposal, including shredding of all paper materials that contain Patient Information (See NIST Special Publication (SP) 800-88, Guidelines for Media Sanitization).

7.4. Participant Privacy and Security Policies & Procedures

Participants shall establish and maintain internal privacy and security policies and procedures that effectively manage access to, and the appropriate use of, Patient Information in compliance with these CORHIO Policies and applicable Laws. Participants shall provide these policies and procedures to CORHIO upon request (See Section 4.3, Participant Policies).

7.5. Data Integrity

Unless specifically authorized, CORHIO, its System Providers, and Participants shall not modify or enrich any Patient Information. CORHIO will employ technical methods, in compliance with applicable Laws, to prevent unauthorized modification of Patient Information while in transmission and at rest on the CORHIO System. CORHIO may enrich or modify Patient Information to support patient matching functions (See Section 6.1.1, Master Patient Index).

CORHIO, its System Providers, and Participants shall ensure that Patient Information is time-stamped and immutable, except where CORHIO has modified or enriched Patient Information, as described above.

7.6. Risk Management

Participants shall periodically conduct a risk analysis to identify the human, natural, technical, and environmental threats to their information systems that contain Patient Information and connect with or may otherwise create risk to the CORHIO System. Participants shall use at least generally-accepted risk management and analysis tools to ensure the security of their systems and processes. Risk assessment should be performed whenever a significant system change is made or at least annually. Participants should consider engaging an independent, third party to assist with or perform the risk assessment.

CORHIO shall create a risk management strategy and annual security plan that will be available to Participants upon request. The strategy and plan shall include disaster recovery procedures, as appropriate.

At least annually, CORHIO and its System Providers shall conduct a global risk assessment to identify the human, natural, technical, and environmental threats to the CORHIO System. This analysis shall include a thorough and comprehensive risk assessment of the sensitivity, vulnerabilities, and security of the CORHIO System and services, as well as the Patient Information that it receives, stores, and distributes. CORHIO shall use at least generally-accepted risk management and analysis tools to ensure the security of its systems and processes. Documentation associated with the risk assessment shall be retained for a minimum of six (6) years and in accordance with applicable Laws.

The risk management strategy will be reviewed, and the risk assessment updated as necessary, such as when a significant change to the CORHIO System is made. CORHIO may engage an independent third party to assist with or perform risk assessments (or require its System Providers to do so), as it deems fit.

7.7. Breach Mitigation

In the event of a known or suspected intrusion or other compromise to the CORHIO System, electronic communication between CORHIO and any affected Participant(s) or Authorized User(s) may be suspended until the issue has been mitigated.

In the event of a data breach, Participants, CORHIO, and its System Providers will take appropriate steps to mitigate the impact of such breach. CORHIO shall assess and must approve any corrective actions to be taken by its System Providers, prior to returning the CORHIO System to normal operations.

7.8. Breach Notification

Participants shall maintain a breach notification process, consistent with applicable Laws, the DURSA, and the operating policies and procedures of the eHealth Exchange (also known as "Healtheway"), to notify CORHIO and other appropriate parties, as required by Law, if a data breach or other security event should occur that affects the CORHIO System or Patient Information. Participant breach notification processes must, at a minimum, comply with applicable Laws and include notification to CORHIO and affected Patients, where appropriate.

CORHIO shall maintain a breach response process, consistent with applicable Laws, its Business Associate Agreements, the DURSA, and the operating policies and procedures of the eHealth Exchange (Healtheway), to notify all Participants and others, as required by Law, if a data breach or other security event should occur that affects the CORHIO System or Patient Information. CORHIO will maintain a list of appropriate contacts (and escalation points) to provide Participants, and others, as appropriate, with such notification, based on an event's characteristics.

Each of CORHIO's System Providers shall maintain a breach response process, consistent with applicable Laws, its agreement(s) with CORHIO, the DURSA, and the operating policies and procedures of the eHealth Exchange (Healtheway), to notify CORHIO if a data breach or other security event should occur that impacts the CORHIO System, Patient Information, or any elements that provide services or are connected to the CORHIO System. Each of CORHIO's System Providers will maintain a list of appropriate contacts (and escalation points) to provide CORHIO with such notification, based on an event's characteristics.

7.9. Extended Policy: Review of Security Policies & Procedures for Participants That Are Not HIPAA Covered Entities

Participants that are not HIPAA Covered Entities are subject to additional review of their security policies and procedures by CORHIO. Prior to providing access to the CORHIO System or Patient Information, CORHIO shall (1) request documentation, conduct interviews with appropriate personnel, and collect other materials, as needed, to reasonably assess such a Participant's security program; and (2) conduct a reasonable review of such a Participant's security program to determine whether it provides for safeguards that are at least as protective of Patient Information as those required by the HIPAA Rules and these CORHIO Policies. CORHIO may seek additional review and guidance from the CORHIO Policy Committee regarding such Participants and their security programs.

8. Extended Policies: HIE Security & System Maintenance Policy

This section establishes additional requirements that CORHIO must meet in implementing, maintaining, and operating the CORHIO System. CORHIO may use contractors to support the CORHIO System and requires that such System Providers adhere to these policies. Accordingly, where these Policies apply to CORHIO, they shall be read as extending to such System Providers. Certain components of these Policies may specifically refer to System Providers for emphasis, clarity, or to provide additional detail. (See Section 3, Scope)

8.1. Transparency & Accountability

CORHIO supports a general policy of openness and transparency about organizational developments, practices, and policies.

CORHIO supports transparency with Participants, Patients, and consumers regarding its services and will facilitate consumer and Patient engagement through their representation in advisory groups, educational programs, and a feedback mechanism for them to ask questions and make suggestions.

On a regular basis, CORHIO shall develop updated information to educate the public regarding the purpose of the CORHIO System, the functions it provides, the security and privacy standards it uses to ensure Patient privacy, and other CORHIO System performance and auditing information. This information shall be provided, at a minimum, on the CORHIO website.

8.2. Security Considerations for Hardware/Software Development & Maintenance

CORHIO and its System Providers shall maintain industry standards for security in the course of developing and maintaining the hardware, software, and services that support the CORHIO System and facilitate CORHIO activities.

8.2.1 Vulnerability Management

CORHIO and its System providers shall maintain a vulnerability management program to regularly review reputable, generally-accepted resources for new technical vulnerability information and periodically perform threat assessments and vulnerability scans across CORHIO System components. CORHIO shall utilize third-party independent assessment organizations, as appropriate. Risk mitigation strategies, such as system patching or configuration changes, shall be developed according to risk and exposure levels using reasonable security practices.

8.3. System Management

The policies in this section help ensure that CORHIO System operations are planned, coordinated, managed, and monitored in a rigorous and consistent manner.

8.3.1 Service Level Agreements (SLAs)

CORHIO shall establish service level agreements (SLAs) with its System Providers and Participants that set minimum transaction processing, system availability, and other variables, as appropriate.

8.3.2 Asset and Configuration Management

CORHIO and its System Providers shall maintain an inventory of CORHIO System components and configurations, including storage media. Asset management processes shall be implemented to track storage media and ensure proper data erasure and equipment disposal as assets are retired.

8.3.3 Backups, Disaster Preparedness, and Emergency Management

Through the annual global risk assessment process (See Section 7.6, Risk Management), CORHIO and its System Providers shall identify and implement processes required to ensure business continuity in the event of an emergency (e.g., system outage, fire, power outage, act of terrorism, or other unforeseen event), including emergency access to the CORHIO System.

8.3.4 Capacity Monitoring

CORHIO and its System Providers shall maintain generally-accepted processes to monitor system capacity and plan for system and network updates required to maintain SLAs, in a timely manner.

8.3.5 System Monitoring and Operations

CORHIO and its System Providers shall support generally-accepted processes to maintain and operate the CORHIO System. Such processes shall include monitoring systems for data integrity, creating and monitoring system activity logs, and ensuring time synchronization across system components.

8.3.6 System and Services Acquisition

CORHIO shall implement processes and procedures to ensure that all hardware, software, and services considered for use in the CORHIO System are capable of satisfying CORHIO Policies for safeguarding privacy and security prior to acquisition.

8.3.7 Technical Support for Participants

CORHIO and its System Providers shall establish processes and procedures to provide technical support for Participants, both at initial implementation and on an ongoing basis, according to SLAs.

8.3.8 CORHIO System Downtime, Maintenance, Updates, and Enhancements

For the CORHIO System to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that the CORHIO System be taken offline or performance degraded temporarily. There may also be security incidents, serious environmental events, or Data corruption/technical errors that give rise to a substantial risk of harm to individuals, that may require CORHIO to take similar action with respect to the entire System or to specific Participants affected by a security or Data corruption/technical error.

Consistent with CORHIO's obligations in the Participant Agreement and SLAs, Participants understand and acknowledge that the HIE may be temporarily unavailable, or performance may be degraded temporarily, for any of the following reasons, including but not limited to:

- Performing routine (e.g., weekly) scheduled maintenance;
- Performing scheduled updates;
- Performing unscheduled maintenance and updates necessary to protect the health IT infrastructure of the HIE and/or to safeguard the confidentiality, integrity, or availability of Data;
- Performing batch updates to patient or member panels or other Data ques necessary to HIE operations;
- Addressing suspected or mitigating known security incidents;
- Implementing CORHIO product or System enhancements;
- As a result of serious environmental or other events; or
- Substantially reducing a risk of harm to the life or physical safety of a natural person, which arises from Data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.