Colorado Health Information Exchange (HIE) Governing Principles & Policies

Version 10.0

September 26, 2023

Contexture Colorado Health Information Exchange Governing Principles & Policies Revision History		
Version	**Date**	**Notes**
10.0	September 26, 2023	Approval by the Contexture Policy Advisory Council on September 7, 2023 and the Contexture Board of Directors on September 26, 2023.
9.0	March 28, 2023	Approval by the Contexture Policy Advisory Council on March 22, 2023 and the Contexture Board of Directors on March 28, 2023
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 Data; • 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 Data 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

This section sets forth the Governing Principles that drive Contexture's Colorado Health Information Exchange (HIE) operations and information practices and which help Contexture to live our mission of *Advancing individual and community health and wellness through the delivery of actional information and analysis*.

These Governing Principles apply to the Colorado HIE operated by CORHIO and its affiliate Contexture, a Colorado non-profit corporation. All references to Contexture should be read to include CORHIO.

1.1 **Openness and Transparency**

Contexture supports a general policy of openness and transparency about developments, practices, and policies impacting the use and disclosure of Protected Health Information (see definition in Section 2) through the HIE. Individuals and Participants should be able to know what Data is maintained by Contexture on behalf of its Participants and the purposes for which Data is used, or can be accessed.. Contexture is committed to facilitating the safe and secure exchange of PHI in a usable format across systems to improve patient care and reduce healthcare costs.

1.2 **Permitted Use and Minimization**

The purpose of the HIE should be explained to individuals at the time their information is initially collected and information should only be obtained by lawful and fair means with the knowledge or consent of the affected individual, where possible. Protected health information should only be exchanged through the HIE for lawful and Permitted Uses and only information necessary for the legally authorized Permitted Uses should be used by Participants.

1.3 **Individual Participation and Privacy Practices**

Individuals have rights regarding Data maintained in the HIE. To support those rights, Contexture has established privacy practices to enable individuals to opt out of having their information available in the HIE and will require its participants to adhere to those practices.

1.4 **Information Integrity and Quality**

All Protected Health Information provided to Contexture should be accurate, current, and relevant to the purpose(s) for which it is to be used.

1.5 **Security Safeguards and Controls**

Contexture will protect health information in the HIE in accordance with industry standards and via reasonable security measures, including administrative, physical, and technical safeguards and controls to protect against risks such as loss, unauthorized access or modification, inadvertent destruction, or inappropriate use or disclosure.

1.6 **Accountability and Oversight**

Entities in control of PHI, including Contexture and its participants, must be held accountable for complying with measures which implement these principles stated above.

1.7 **Compliance with Applicable Laws & Support for Emerging Standards and Practices**

Contexture 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 Contexture COLORADO 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 Contexture Colorado 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.

1. Actor

"Actor" means a healthcare provider (as defined in 42 U.S.C. § 300jj), a health IT developer of certified health IT (CHIT Developer) or a health information network (HIN)/health information exchange (HIE), all as defined by the Information Blocking Rule at 45 C.F.R. § 171.102.

2. 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 Contexture for implementation and operational purposes.

3. Authorized User

"Authorized User" means the following:

- An individual approved and identified to Contexture, by a Participant, to use the Contexture 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 Data provided by the Contexture System through a system-to-system level interface (the Participant is responsible for approving, identifying, and authenticating such Authorized Users); or
- A Contexture Workforce Member whose role requires access to the Contexture System.

4. Community Health Record

"Community Health Record" means a set of Data 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 Contexture System.

5. Contexture

"Contexture" means the Colorado non-profit corporation that is the sole controlling member of the Colorado Regional Health Information Organization ("CORHIO"), itself a Colorado nonprofit organization. When the term Contexture is used in this policy, it refers to both itself and its joint venture affiliate, CORHIO.

6. Contexture Policy Advisory Council

"Contexture Policy Advisory Council" means the multi-stakeholder advisory council established

by Contexture to provide advice and recommendations to Contexture and the Contexture Board of Directors regarding these Policies. Policy Advisory Council members represent a variety of stakeholders across Contexture states and healthcare sectors and specialties including various Participant types, government organizations, patient advocacy groups, and other interested parties.

7. ***Contexture Policies***

"Contexture Policies" or "Policies" means these Contexture Colorado Health Information Exchange Governing Principles & Policies and all Procedures established thereunder. These Policies apply only to the operation of the Contexture Health Information Exchange in Colorado and do not apply to the operation of Contexture's separate Health Information Exchange in Arizona.

8. ***Colorado HIE Procedures***

"Colorado HIE Procedures" or "Procedures" means the rules, guidelines, and operational processes and procedures that Contexture may, in its sole discretion, define and adopt to implement these Policies or to otherwise maintain the privacy, security, confidentiality, integrity, and availability of the Contexture System. Colorado HIE Procedures are provided to HIE Participants at implementation and Participants may request a copy of the Colorado HIE Procedures from Contexture.

9. ***Contexture System***

"Contexture System" means Contexture's Internet-based authenticated system and search engine for patient health, demographic, and related information that facilitates the sharing and aggregation of Data held by Participants with disparate health information systems, also known as "health information exchange (HIE)." The Contexture System allows Authorized Users to communicate over a trusted network to access Data. The Contexture 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 Contexture System shall, at a minimum, conform to accepted nationwide standards for the interoperability of health information technology systems and health information exchange.

10. ***Credential***

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

11. ***Data***

"Data" means any individually identifiable information transmitted to Contexture by Data Providers in connection with HIE services, including but not limited to protected health information (PHI). Due to current technical and administrative limitations, it is not feasible for Contexture to distinguish between Data that is and is not PHI. Thus, for purposes of this HIE Policies, all Data accessible through the HIE is treated as PHI.

12. ***Data Feed***

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

13. ***Data Provider***

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

14. ***Data Query***

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

15. ***Data Recipient***

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

16. ***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 Contexture, must join in the DURSA before they can participate in the public-private partnership maintained and operated eHealth Exchange.

17. ***Direct Exchange***

"Direct Exchange" means the transmission and receipt (i.e., exchange) of Data 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 Contexture System.

18. ***Electronic Health Information (EHI)***

"Electronic Health Information" or "EHI" means electronic protected health information (ePHI) contained in a Designated Record Set (DRS), regardless of whether the group of records are used or maintained by or for a covered entity, as those terms are defined by HIPAA. EHI may encompass medical and billing records, health plan records, and other records used to make decisions about individuals when such records are maintained by a healthcare provider, CHIT Developer, HIN or HIE. EHI specifically excludes psychotherapy notes or information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding. EHI also excludes data de-identified in accordance with the HIPAA.

19. ***EHR Interface***

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

20. ***Information Blocking***

"Information Blocking" refers to practices (i.e., acts or omissions) that are likely to prevent, materially discourage or otherwise inhibit (i.e., to interfere with) the access, exchange or use of EHI, including: i) the ability or means necessary to make EHI available for exchange or use (i.e., access to EHI); ii) the ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks (i.e., exchange of EHI); and/or iii) the ability for EHI, once accessed or exchanged, to be understood and acted upon (i.e. use of EHI).

21. ***Information Blocking Rule***

"Information Blocking Rule" collectively refers to 42 U.S.C. § 300jj-52 and its implementing regulations 45 C.F.R. Part 171.

22. ***HHS***

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

23. ***HIE***

"HIE" means health information exchange and may be used as either a noun or verb. Please note that for purposes of the No Information Blocking Policy in Section 8, the term HIE has the meaning set forth in 45 C.F.R. § 171.10.

24. ***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").

25. ***HIPAA Authorization***

"HIPAA Authorization" means a form that meets HIPAA's requirements for a valid authorization form.

26. ***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.

27. ***Lab Report***

"Lab Report" means an electronic record of lab testing results that (1) is transmitted, stored, managed, or otherwise made available through the Contexture 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.

28. ***Law***

"Law" means any federal, state and local 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.

29. ***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).

30. ***Part 2***

"Part 2" collectively refers to 42 U.S.C. § 290dd-2 and its implementing regulations located at 42 C.F.R. Part 2.

31. ***Consent Form***

"Consent Form" means a form approved by Contexture for accessing Part 2 Data through the HIE and that meets Part 2's consent requirements.

32. ***Part 2 Data or "Sensitive SUD Data"***

"Part 2 Data" or "Sensitive SUD Data" means information subject to and protected by Part 2, including without limitation Data that is not itself subject to Part 2 but which cannot feasibly be segmented from Data that is protected by Part 2.

33. ***Part 2 Program***

"Part 2 Program," as defined by Part 2, is a federally assisted individual or entity (including an identified unit within a general medical facility) that holds itself out as providing, and provides, substance use disorder treatment. A Part 2 Program also includes federally assisted medical personnel or staff in a general medical facility whose primary function is providing substance use disorder treatment and who are identified as such providers. A Participant is federally-assisted if it is run in whole or part by the federal government, is carried out under a license or other authorization granted by the federal government (including an authorization to prescribe, order or dispense controlled substances for substance use disorder treatment), is supported by federal funds, or is a 501(c)(3) non-profit organization or otherwise assisted by the IRS with income tax deductions for contributions to the program or through the granting of tax exempt status.

34. ***Participant***

"Participant" means an individual or entity that has entered into a written agreement with Contexture to act as a Data Provider, Data Recipient, or both. 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.

35. ***Participant Agreement***

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

36. ***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.

37. ***Permitted Use***

"Permitted Use" means the specific reasons for which Participants may access data through the HIE, and for which Contexture may use and disclose Data in the operation of the HIE.

38. ***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 Contexture or a Participant in connection with the Contexture System.

39. ***Record***

"Record" means a specific set of Data accessed or assembled through the Contexture System.

40. ***Required by Law***

"Required by Law" means a practice that is explicitly required by State or Federal law, including statutes, regulations, court orders, binding administrative decisions or settlements, as well as tribal law (as applicable). Required by Law does not mean practices permitted by law or engaged in pursuant to a law (such as privacy laws that require an individual's consent or authorization prior to disclosing EHI to the requestor).

41. ***Safe Harbor***

"Safe Harbor" refers to a regulatory exception to the Information Blocking Rule, see 45 C.F.R.

Part 171.

42. ***System Interface***

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

43. ***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 Contexture as support for any part of the Contexture System.

44. ***"Treating Provider Relationship"***

"Treating Provider Relationship" has the meaning defined in Part 2. See 42 C.F.R. § 2.11.

45. ***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.

46. ***Workforce Member***

"Workforce Member" means, as to Contexture 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 Contexture Policies.

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

- Participants, including each Participant's Authorized Person(s)/Point(s) of Contact, its Authorized Users, its Workforce Members, and its designated business associates that are permitted in writing to access the HIE on behalf of the Participant;
- CORHIO, Contexture and its Workforce Members; and
- CORHIO's System Providers, Contexture's System Providers (as applicable), System Provider Workforce Members, and others acting as agents or subcontractors on behalf of a System Provider regarding the Contexture System.

3.2 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.

3.3 Where these Policies apply to CORHIO, they shall be read as extending to Contexture. Any reference to "CORHIO" in these Policies includes Contexture's Workforce Members. Contexture requires that System Providers adhere to these Policies, where applicable. Accordingly, where these Policies apply to Contexture, 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.

3.4 In furtherance of these Contexture Policies, Contexture may, in its sole discretion, define and distribute additional detailed processes or procedures to maintain the privacy, security, confidentiality, integrity, and availability of the Contexture HIE System.

4. Compliance with Law & Policies

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

4.1 **Laws**

Contexture and Participants shall, at all times, comply with all Laws, including those that protect the privacy and security of Data and establish certain individual privacy rights (e.g., HIPAA, HITECH). Contexture 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 **Contexture Policies**

Contexture and Participants shall, at all times, comply with all applicable Contexture Policies. These Contexture 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 Contexture Policies.

4.2.1 **Policy Review**

1. These Policies shall be reviewed from time to time, but not less often than annually, by Contexture and the Contexture Policy Advisory Council. The Council shall submit any proposed revisions to the Contexture Board of Directors for review and approval.
2. The Contexture 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, Contexture will periodically perform a survey and analysis of generally-accepted industry standards and Laws that may impact these Contexture Policies.

4.3 **Participant Policies**

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

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

4.3.3 Participants shall refer to and comply with their own internal policies and procedures regarding Data 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**

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

4.4.2 To ensure compliance with these Contexture Policies, Contexture 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. In instances where providing requested information is infeasible, Participants shall provide access to the requested information in a mutually-agreed upon manner.

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

4.5 **Participant Authorized Person/Point of Contact**

Participants must designate at least one Authorized Person/Point of Contact, who must be recognized by Contexture 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 Contexture on the Participant's behalf and is responsible for ensuring compliance with any applicable agreements, such as the Participant Agreement, and these Contexture Policies. The Point of Contact shall be prepared to interact with Contexture and help coordinate risk mitigation and security event (e.g., data breach, unauthorized use investigation) activities.

4.6 **Training and Acknowledgement**

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

4.6.2 Participants shall maintain documentation regarding their training and acknowledgement process in accordance with these Contexture Policies and applicable Laws.

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

4.6.4 Contexture shall institute a training process for its Workforce Members to ensure compliance with these Contexture Policies.

4.7 **Reporting Non-Compliance**

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

4.7.1 **Sanctions for Non-Compliance**

1. Participants who fail to comply with these Contexture Policies shall be subject to review by Contexture and may have access to the Contexture System terminated.
2. Considering the highly sensitive nature of Data that flows through the HIE System, Contexture maintains a zero-tolerance policy regarding inappropriate or unauthorized use of the Contexture System. Authorized Users who violate these Contexture Policies, as identified through reporting, auditing, or other processes, may be sanctioned as defined in the Contexture 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 Authorized Users accountable for complying with these Contexture Policies and ensuring that they do not access, use, disclose, or request Data except as permitted by these Contexture Policies. If non-compliance occurs, Contexture shall be notified and the individual's access may be terminated, according to the sanctions defined in the Contexture Procedures. Participants may choose to take additional actions according to their own sanctioning policies.
4. All Contexture Workforce Members shall be accountable for ensuring that they comply with these Contexture Policies and do not use, disclose, or request Data except as permitted by these Contexture 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.

4.8 Communications with Other HIEs and Healthcare Organizations

Contexture may enter into agreements that enable health information exchange across different states, regions, communities, and with other healthcare organizations. Such agreements may expand Contexture's reach and provide data exchanges with the participants of other HIEs. Contexture shall be responsible for confirming that the policies of such other HIEs and healthcare organizations are at least as protective of Data as specified in these Contexture 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).

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

1. Contexture or its joint venture affiliate CORHIO is 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 Contexture, 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" Contexture 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 Contexture Policies and reaffirms the obligations of Contexture and its Participants to comply with applicable Laws (e.g., HIPAA, state and federal privacy and security statutes and regulations). Contexture Participants must recognize that they are part of this broader HIE community as a result of Contexture's participation in the DURSA and the eHealth Exchange. To that end, Contexture 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 Data exchanged through the eHealth Exchange.
3. Contexture Participants must (1) reasonably cooperate with Contexture on issues related to the DURSA; (2) exchange Data through the eHealth Exchange only for a "permitted purpose" as defined by these Contexture Policies and the DURSA; (3) use Data received through the eHealth Exchange only in accordance with the terms of the DURSA; and (4) notify Contexture as soon

as reasonably practicable after determining that a data breach has occurred, so that Contexture 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, Contexture 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 Permitted Use and User Access

Section 5 applies to Contexture and its Participants. Due to legal, technical and operational limitations, access to the HIE is currently limited to Participants that are:

- Health Care Providers and their designated Business Associates;
- Health Plans and their designated Business Associates;
- Public Health Authorities;
- Medical Examiners;
- Organ Procurement Organizations;
- Approved Government Agencies; and
- Insurance Companies.

Each type of Participant may only access Data for the Permitted Uses that apply to them. Contexture may also use and disclose Data for the Permitted Uses set forth in this policy. Once Data from the Contexture HIE 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 own policies and procedures. This section also defines how access to the Contexture System is established and contains Contexture's Policies related to patient access and auditing.

5.1. **Colorado HIE Permitted Use Policy**

Participation in the Contexture HIE is limited to the following Participant Types.

5.1.1. **Health Care Providers**

Participants that are HIPAA Covered Entity Health Care Providers, as defined at 45 CFR § 160.103, and their designated Business Associates may access Data through the HIE for the following Permitted Uses: **Treatment, Payment, and Limited Healthcare Operations.** Participants that are Health Care Providers, but are not Covered Entities, as defined at 45 CFR § 160.103, may access Data through the HIE for the following Permitted Uses: **Treatment and Payment**.

For Treatment and Payment Permitted Uses, Access is permitted for Data of individuals who are current patients of the Health Care Provider, prospective patients with whom the Health Care Provider is expected to establish a treatment relationship, and past patients for whom the Health Care Provider is transitioning to a new Health Care Provider. For Limited Healthcare Operations Permitted Uses, access is permitted for Data of individuals who are current or past patients of the Health Care Provider.

The HIPAA minimum necessary standard applies to the Payment and Limited Healthcare Operations use cases. To comply with the minimum necessary standard, the Healthcare Provider Participant (or Business Associate) will limit its requests to only the Data needed for the Health Care Provider to conduct the Payment or Limited Healthcare Operations activities.

5.1.2. **Health Plans**

Participants that are Health Plans, as defined at 45 CFR § 160.103, may access data through the HIE for Payment and Limited Healthcare Operations. Access is permitted for Data of individuals who are currently enrolled members with the Health Plan and for past members for whom the Health Plan is transitioning to a new Health Plan. Health Plans may also access Data of prospective members seeking to enroll in the Health Plan, if necessary, for Payment purposes.

Regardless of whether permitted by Law, the following uses of Data are prohibited:

- 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 Contexture and a Government Agency Participant.

The HIPAA minimum necessary standard applies to the Payment and Limited Healthcare Operations use cases. To comply with the minimum necessary standard, the Health Plan Participant (or Business Associate) will limit its request to only the Data relevant to the Payment or Limited Healthcare Operations activities.

5.1.3. **Public Health Authorities**

A Public Health Authority (PHA), as defined at 45 CFR 164.501, may access data to conduct legally authorized Public Health Activities, as permitted by 45 CFR 164.512, 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. The PHA is permitted to access Data only of individuals who are the subject of a Limited Public Health Activity.

The HIPAA minimum necessary standard applies to the Public Health Activity use case. To comply with the minimum necessary standard, a Public Health Authority will limit its request to only the Data needed for a Public Health Activity. Contexture may reasonably rely on a minimum necessary determination made by the public health authority in requesting the PHI.

5.1.4. **Coroners and Medical Examiners**

Coroners and Medical Examiners may access Data through the HIE for uses and disclosures for death evaluation purposes permitted by applicable state law in Colorado, including identifying a deceased person, determining a cause of death, conducting a death investigation, and performing other duties as authorized by applicable Laws. Coroners and Medical Examiners may only access the Data of a decedent who is the subject of a death evaluation. The HIPAA minimum necessary standard applies to the Coroners and Medical Examiner use case. To comply with the minimum necessary standard, the Coroner or Medical Examiner will limit its request to only the Data needed for the Coroner or Medical Examiner Activity.

5.1.5. **Organ Procurement Organizations**

Federally sanctioned Organ Procurement Organizations may access Data for the purpose of facilitating organ, eye or tissue donation and transplantation as permitted by applicable Laws. Access is permitted for Data of individuals who are donors or prospective donors of their organ(s), eye(s) or tissue(s). The HIPAA minimum necessary standard applies to the organ procurement use case. To comply with the minimum necessary standard, Organ Procurement Organizations will limit their request to only the Data needed for the organ, tissue, or eye procurement activity.

5.1.6. **Government Agencies**

Government Agencies means Federal, state, and local government agencies that are not Health Care Providers and are not Public Health Authorities or Correctional Institutions and that have been approved in advance by Contexture. Government Agencies may only access Data through the HIE pursuant to a valid HIPAA Authorization as permitted by HIPAA. Access is only permitted for Permitted Uses that are authorized by law. Contexture will refer any requests for Data for judicial proceedings or law enforcement purposes, to the applicable Data Provider(s) consistent with these Policies (see section 5.3.2, Use Purposes).

5.1.7. **Correctional Institutions**

Correctional Institutions, as defined by 45 CFR 164.501, may access Data through the HIE for custodial situations permitted by 45 CFR 164.512(k)(5) and CRS § 27-70-101 *et. seq.* A Health Care Provider at a correctional institution may access Data through the HIE of individuals who are inmates in accordance with the Health Care Provider Permitted Use Policy in Section 5.1.1. Contexture will refer any requests for Patient Information for judicial proceedings or law enforcement purposes, to the applicable Data Provider(s) consistent with these Policies (see section 5.3.2, Use Purposes).

5.1.8. **Insurance Companies**

Insurance Companies means entities (other than Health Plans) that offer insurance products, such as life insurance, disability, and long-term care insurance. Contexture may provide access to authorized Insurance Companies pursuant to a Patient Authorization (As permitted by 45 CFR 164.508(a)(1)) obtained and maintained by participant prior to HIE access.

Each type of Participant may only access data for the Permitted Uses that apply to them. Participants shall make reasonable efforts to only access or request only the minimum necessary PHI available through the HIE to accomplish the intended purpose (as described in 45 C.F.R. 164.502(b) and 164.514(d)). Once data from the HIE is accessed by a Participant or their Business Associate 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 Laws and Participant's own policies and procedures. Participants and their Business Associates will comply with their own minimum necessary standard policies and procedures, as well as any other restrictions set forth herein, in connection with their use of HIE services.

In addition, Contexture may disclose patient information to a Participant pursuant to a valid HIPAA Authorization if Contexture has the appropriate technical and administrative processes in place to support an authorized recipient's access in accordance with Applicable Laws and healthcare industry standard security practices.

5.2. User Authorization

Access to the Contexture System and Data is limited to Authorized Users.

5.2.1. Secure Access, Authorization, and Authentication

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

2. Contexture shall provide Participants with Credentials for Authorized Users who utilize Contexture-supplied end user interface components. Contexture 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 5.2.3, Changes to Authorized Users). Contexture shall establish terms and conditions for log-in using Contexture-supplied Credentials, including requirement for multi-factor authentication access to the Contexture System. Detailed rules regarding strong passwords, access suspension, password expiration, password caching, and automatic log off shall be provided in the Contexture 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 Contexture System will also authenticate the requesting organization using agreed upon technical standards at the time a request is made. To the extent technically feasible, Contexture 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.

5.2.2 **Authorized User Identification**

Contexture and Participants shall allow access to the Contexture System only by those Workforce Members who have a legitimate and appropriate need to use the Contexture System or release or obtain Data through the Contexture System. No Workforce Member shall be provided with access to the Contexture System or Data obtained from it without first having been trained on these Contexture Policies, to the extent applicable (See Section 4.6, Training and Acknowledgement).

Each Participant's Point of Contact shall identify those to be treated as Authorized Users by Contexture, 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 Contexture System for Permitted Uses set forth in Section 5.1 and in accordance with the Appropriate Use Policies in Section 5.3 (See Section 5.3, Appropriate Use & Disclosure).

5.2.3 **Changes to Authorized Users**

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

1. **Change Includes Authorized User Disciplinary Action**

   If a change relates to an Authorized User who has been disciplined for using, disclosing, or requesting Data in a manner not permitted by these Contexture Policies or in violation of applicable Laws or these Contexture Policies, Participant shall notify Contexture immediately, and under no circumstances, later than 24 hours following the change in Authorized User status. This notification may be followed by sanctions against the non-compliant individual or Participant, as defined in the Contexture Procedures.

2. **Change Does Not Include Authorized User Disciplinary Action**

   If a change to an Authorized User status is not related to non-compliance with applicable Laws or these Contexture Policies (if the Authorized User is no longer a Workforce Member of Participant), then the Participant shall notify Contexture as soon as possible, and no later than 72 hours, so that Contexture can take appropriate steps to remove credentialed access for that Authorized User.

5.2.4 **No Log-In/Password Sharing**

Contexture 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 Colorado HIE Procedures.

5.3. **Appropriate Use & Disclosure**

Data available through the Contexture System may only be used and disclosed in a manner that is consistent with applicable Laws and these Contexture Policies. Data Providers are responsible for ensuring that a proper HIPAA Authorization, if required by Law, is obtained prior to sharing Data for use and disclosure through the Contexture System. Any Data supplied by a Data Provider will be deemed to be authorized for sharing through the Contexture System unless the Data Provider indicates in writing to Contexture that the

Patient has opted out of sharing (See Section 6.3, Patient Participation and Choice Not to Use the Contexture System ("Opt-Out")).

5.3.1 **Appropriate Use**

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

5.3.2 **Use Purposes**

1. Participants shall provide or request Data through the Contexture System only for purposes permitted by Law, the Participant Agreement and these Contexture Policies. Data may only be requested and shared through the Contexture 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 Data through the Contexture System for Permitted Uses as described in these Policies. In the absence of a permitted use, Participants shall not access Data through the Contexture System. Regardless of whether permitted by Law, the following uses of Data are prohibited:

- Any Marketing purposes;
- Any Fundraising purposes;

3. If Contexture or any of its subcontractors or third party vendors receives a court order or subpoena for Data, or a request for Data by a government entity pursuant to applicable Law, Contexture, to the extent permitted by applicable Law, will provide timely notice to the Participant that provided the Data, 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). Contexture 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 Contexture. Contexture will comply with applicable Law, including Colo. R. Civ. Proc. 45, in responding to subpoenas.

5.3.3 **Use & Disclosure of Laboratory Test Results**

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

5.3.4 **No Discrimination**

Contexture does not permit the use of Data for unlawful discriminatory purposes. Under no circumstances shall Data be accessed or disclosed for an unlawful discriminatory purpose. If and when Contexture should become aware that Data 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 Contexture Procedures.

5.3.5 **Incorrect or Inappropriate Use or Disclosure**

In the event that Data is used or disclosed for other than Permitted Uses, Contexture 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 Contexture's policies.

5.3.6 **Data Subject to Special Protection**

Federal and state laws impose heightened privacy and security requirements upon the disclosure of certain types of Data that may be considered particularly private or sensitive (e.g., alcohol and substance abuse treatment records subject to 42 C.F.R. Part 2, psychotherapy notes, services paid for out-of-pocket when requested). Any disclosure of Data must be conducted in compliance with all applicable Laws. Data Providers are responsible for complying with such Laws and shall determine what (if any) Data is subject to special protection prior to making it available through the Contexture System. Please see sections 5.4 and 5.5 regarding 42 C.F.R. Part 2.

5.4. **Part 2 Data Submissions**

CORHIO has enhanced its HIE System to support its HIE participants' Data Exchange involving Part 2 Data based on an active Consent Form or in certain medical emergency situations. Federal law gives greater privacy protections to Part 2 Data. Contexture must restrict Part 2 Data from displaying in the HIE and through other Data services to comply with these more restrictive requirements. Due to current technical limitations and medical record keeping practices, it is often not feasible for Contexture to separate Part 2 Data from other Data supplied by Part 2 Programs. Contexture thus restricts all Data from Data Providers that operate Part 2 Programs from commingling with other Data accessible through the HIE unless the Data Provider can segment the Part 2 Data from the other Data appropriately.

Before submitting any Data to the HIE, Data Providers must notify Contexture in writing if they operate a Part 2 Program or are in possession of Part 2 Data so that Contexture can properly restrict the Data.

5.5. **Part 2 Data Access**

Part 2 gives heightened privacy protections to Part 2 Data. Due to current technical and administrative limitations on the ability to segment Part 2 Data from other Data and as explained in these Policies, Contexture restricts all Data from Part 2 Programs from being commingled with other Data in the HIE and protects it in accordance with Part 2.

Participant may access Part 2 Data under the following circumstances:

5.5.1 **Consent Form**

Participants may access Part 2 Data through the HIE pursuant to a Consent Form. Contexture requires use of an approved Consent Form because this is the only feasible option available to Contexture for compliance with Part 2's complex consent and related requirements (e.g., prohibition on redisclosure notice) in the HIE environment given current technical, administrative and financial constraints. Participants must also follow all of Contexture's technical and administrative processes related to documenting consent.

Any document uploaded to the HIE System in order to apply consent-based access to Part 2 Data must meet all of the following requirements: (a) the document uploaded is a Contexture Consent Form signed and dated by the Patient who is the subject of the Part 2 Data and, when required for a Patient who is a minor, the signature of an individual authorized to give consent under 42 C.F.R. § 2.14, or, when required for a Patient who is incompetent or deceased, the signature of an Individual authorized to sign under 45 C.F.R. § 2.15; (b) the Consent Form has not expired; (c) the Consent Form is not known to have been revoked; (d) the Consent Form substantially conforms to Part 2 consent requirements; and (e) the Consent Form is not known to Participant, or through reasonable diligence could not be known, by Participant to be materially false.

Use of any other Consent Form other than Contexture's branded and authorized Consent Form is prohibited unless the alternative consent form has been approved in writing by Contexture's Legal Department.

Participant is required i) to verify the identity and authority of the Individual(s) who signed the Consent Form using healthcare industry standard security measures; ii) to enter the correct expiration date of the Consent Form into the HIE System; and (iii) to maintain copies of such Consent Forms for at least six (6) years after expiration of the Consent Form.

Only Authorized Users with a Treating Provider Relationship with the Patient who is the subject of the Part 2 Data may access Part 2 Data in the HIE System based on active Consent Form. Participant will ensure that only those Authorized Users with appropriate roles within its organization who are legally eligible to access Part 2 Data pursuant to the Patient's Consent Form may have access to the Part 2 Data. Authorized Users may only access the Sensitive SUD Data on the HIE System for Treatment, Payment and Limited Healthcare Operations purposes.

Contexture will maintain an accounting of disclosures made pursuant to the Consent Form and, upon a validated Patient request, provide a listing of disclosures required by Part 2 to the Patient. Participant acknowledges and agrees that Contexture may provide this information directly to the Patient without further consent or agreement from Participant.

5.5.2 **Medical Emergency Access**

Only Authorized Users who are medical personnel may request and access Part 2 Data using the medical emergency functionality. Participant must ensure that their Authorized Users only use the medical emergency functionality if they have determined in good faith and using their professional judgment that such access is necessary to meet a bona fide medical emergency in which the Patient's Consent Form cannot be obtained. For clarity, if a Patient has legal capacity to consent and chooses not to give consent (for example, choosing not to sign the Consent Form), Participant and its Authorized Users cannot use the medical emergency functionality to access the Patient's Part 2 Data. Authorized Users must document the nature of the medical emergency in the Patient's medical record and HIE System.

Authorized Users who request medical emergency access to Part 2 Data shall provide all the information required by the HIE System or requested from Contexture to support documentation of the medical emergency access. Authorized Users may be denied access to the Part 2 Data if they do not provide the requested information.

5.5.3 **Case-by-Case Determinations**

Participants may request in writing that Contexture provide access to Part 2 Data for other Permitted Uses. Contexture will determine on a case-by-case basis whether it is feasible for Contexture to provide the requested access and whether access is permitted under Part 2 and any other applicable Laws.

5.5.4 **General Requirements for Part 2 Data Access**

5.5.4.1 Data Use Restrictions. Contexture may: (a) impose its own role-based access restrictions on the types of Authorized Users who may access Part 2 Data and use the Part 2 Data Services, in order to support Contexture's and its participants' compliance with Applicable Law; and (b) require Authorized Users to provide additional attestations or agree to additional terms and conditions in connection with their use of the Part 2 Data Services (collectively,

"User Terms"). Contexture may prohibit an Authorized User from accessing Sensitive SUD Data if the Authorized User does not agree to the User Terms.

5.5.4.2 Audit. Contexture may inspect and audit Participant's records relating to its compliance with the terms of the Addendum, including but not limited to Sensitive Data Source status, Consent Forms, and reasons for medical emergency access. Participant may impose reasonable restrictions upon CORHIO's access to its premises and information systems. All audits shall be conducted with the least interruption to Participant's normal business operations as is reasonably feasible.

5.6 Patient Participation and Access to the Contexture 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 Contexture does not have a direct relationship with individuals whose Data is accessible through the HIE, Contexture relies on Participants to manage relationships and disclosures of Data from the Contexture System to Patients. Patients who contact Contexture regarding their Data shall be referred to one or more of the Participants where they receive care. Due to legal, technical, and administrative limitations, the Contexture 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. Contexture may pilot or develop projects to facilitate Patient access to Data available through the Contexture System, but such functions will require approval, involvement, and/or action on the part of interested Participants.

5.7 Auditing

Contexture has the right to audit Participant's use of the Contexture System to ensure compliance with Participant Agreements, other applicable agreements, and these Contexture Policies. In addition, security administration functions, system administration functions, and other system-level activities of the Contexture System will be logged and monitored.

5.7.1 Audit Log

The Contexture 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.

Contexture will make audit log information available to Participants upon written request for purposes such as responding to Patient requests, managing compliance, and conducting investigations.

5.7.2 Audit Log Controls

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

5.7.3 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.

5.7.4 System Audits

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

Contexture may periodically activate, facilitate, or conduct system audits to review Authorized User or system activities. Participants may request audits of their specific Authorized Users or activities.

6. Privacy Practices

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

6.1 **Patient Identification**

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

6.1.1 **Master Patient Index**

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

1. **Computer-Based Matching System**

   Contexture 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.

2. **Usage Limitation on Social Security Number and Government-Approved Identification Numbers**

   Subject to applicable Laws, Contexture 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.

6.1.2 **Patient Query**

An Authorized User shall query the MPI and view Patient demographic information only in accordance with these Contexture Policies. When searching the MPI, Authorized Users must provide, at a minimum, the mandatory data fields, as required by the Colorado HIE 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 Data, as described in the Colorado HIE Procedures.

6.1.3 **Action Required for Incorrect Match**

Participants shall report search results that indicate an incorrect Patient match has occurred to Contexture on an as soon as possible basis. Contexture 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 Data received from Contexture does not apply to the Patient about whom information was requested, the Authorized User shall take reasonable steps to immediately destroy that Data, including, where applicable, deleting the Data received from Contexture and properly disposing of any paper or electronic copies. The Authorized User shall contact Contexture, or the appropriate Authorized Person / Point of Contact who shall alert Contexture to the occurrence. Contexture will maintain records, including audit logs, as required by these Contexture Policies and Law, and will follow its breach response procedures, as appropriate.

6.2 Informing Patients of Contexture Participation

Participants that are Health Care Providers and Health Plans shall maintain a Patient notification process (or, as applicable, a HIPAA 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. Contexture will provide Participants with a sample Patient notification document that complies with these Contexture Policies. Participants shall have the option to either use the Contexture-provided sample or incorporate the information provided by Contexture into their own Patient notification process (the "Contexture CO HIE Notice").

Participants shall have their own policies and procedures governing distribution of the Contexture CO HIE Notice to Patients, which shall comply with these Contexture Policies and all applicable Laws, including the HIPAA Rules. For the avoidance of doubt, a Participant that is a Health Care Provider is required to distribute the CO HIE Notice if i) the Health Care Provider (or its Business Associate) makes Data generated or maintained by the Health Care Provider accessible through the HIE, or ii) the Health Care Provider accesses Data directly through the HIE System.

Notice Content

The CO HIE Notice shall meet the content requirements set forth under the HIPAA Rules and otherwise comply with all applicable Laws. The CO HIE Notice also shall include a description of the Contexture System and inform Patients regarding: (1) what information the Participant may include in and make available through the Contexture System; (2) who is able to access the information through the Contexture 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 Contexture System.

6.3 Patient Participation and Choice Not to Use the Contexture 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 Data to be shared through the Contexture 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 Contexture System and subject to sanctions.

6.3.1 Patient Choice Processes

Participants and Contexture 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 Contexture System. Participants retain the responsibility for determining the specific process by which patients may exercise their choice.

Contexture shall also establish and maintain a secondary process to allow Patients to choose not to have Data made available through the Contexture System, other than for Direct Exchange between Participants with whom the Patient has an established relationship. Contexture 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 Contexture System may be exercised through the Participant, as described in the Participant's CO HIE Notice or through a secondary process supported by Contexture. A Patient's choice to not share information through the Contexture 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 Data among Participants with which the Patient has an established relationship, also known as Direct Exchange, may still take place through the Contexture System.

6.3.3 Opt-Out Revocation

A Patient who has chosen to opt-out of information sharing through the Contexture System may subsequently choose to allow sharing of his or her Data 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 Contexture.

6.3.4 Patient Choice Documentation

Contexture and Participants shall document and maintain such documentation of all Patients' decisions not to have Data shared through the Contexture System and any revocations of such decisions, for a minimum of six (6) years and in accordance with all applicable Laws. Participants shall inform Contexture of Patients' choices according to methods established in the CO HIE Procedures. For audit or review purposes, Contexture 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. To assist Participants in fulfilling their accounting of disclosures requirements to Patients, Contexture shall maintain logs of uses and disclosures of Data through the HIE System in accordance with Section 5.5 and with the applicable Business Associate Agreement. If contacted directly by a Patient, Contexture shall direct the Patient to contact one or more of the Participants where they receive care.

6.5 Amendments to Patient Records

Contexture shall not make changes to Patient Records in response to a request for amendment from a Patient or individual. 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 Contexture for the purpose of notifying other Participants as may be required to comply with the HIPAA Rules.

7. HIE Security and Maintenance

Contexture and Participants are committed to Contexture System data security. This section describes the security and maintenance practices that are reasonable and necessary to protect the confidentiality, integrity, and availability of the Data that is created, received, transmitted, stored, or otherwise managed by the Contexture System, and to maintain and improve the health IT performance of the HIE.

7.1. **Security Procedures**

Contexture's cybersecurity policies and processes establish appropriate security controls, including administrative, physical, and technical safeguards. In connection with HIE services, Contexture and Participants will use administrative, physical, and technical security measures—such as access controls, authentication measures, auditing procedures and security incident reporting—that meet applicable legal requirements, security and reporting obligations in the Participant Agreement, and best security practices in the healthcare industry.

Participants must also follow Contexture's security protocols and related measures, with respect to Participants' use of HIE services, such as minimum username/password requirements, authentication procedures, and access termination requirements. These security measures are all directly related to safeguarding the confidentiality and integrity of Contexture System data by mitigating the risk of access by unauthorized persons, see 45 C.F.R. 164 Subpart C.

7.2. **Secure Infrastructure**

Contexture, its System Providers, and Participants shall only allow Authorized Users and Contexture System operations personnel to access the Contexture System from secured end user environments. Contexture shall provide technical security specifications to Participants as part of the implementation process. As a condition of implementation and to support ongoing risk assessment, Contexture may request a network component diagram and standard documentation from Participants to ensure that appropriate hardware and software have been implemented and are maintained on an ongoing basis.

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

7.3 **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, Data in compliance with these Contexture Policies and applicable Laws. Participants shall provide these policies and procedures to Contexture upon request (See Section 4.3, Participant Policies).

7.4 **Risk Management**

Participants shall periodically conduct a risk analysis to identify the human, natural, technical, and environmental threats to their information systems that contain Data and connect with or may otherwise create risk to the Contexture 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.

7.5 **Requirements for Patient Panel and Member File Submissions**

Some HIE services (i.e., Notifications and certain HIE reporting services) require Participants or their designated Business Associates to supply Contexture with an up-to-date patient panel or member file for attributed individuals (collectively, "Patient Panels"), which Contexture utilizes to route Data to Participants in accordance with the Permitted Use Policy. Such Participants and Business Associates must submit Patient Panels in accordance with the following requirements.

1. All Participants and Business Associates must submit Patient Panels that comply with Contexture's standard Patient Panel specifications, which are supplied during the HIE implementation process. By including an individual on the Patient Panel, the Participant or Business Associate represents that the Participant has a current HIPAA-compliant Treatment, Payment or Limited Healthcare Operations relationship with the individual.
2. After the submission of an initial Patient Panel, all Participants and Business Associates must update and refresh such Patient Panels via submission of a delta file that indicates which individuals should be added or deleted from Participant's Patient Panel and follows the standard specification for delta file submissions provided by Contexture during implementation. If a Participant does not have the technical ability to update a Patient Panel via submission of a delta file, then such Participant must receive written approval from Contexture to submit updates to a Patient Panel via an alternative method.
3. Health Plans and their Business Associates must update their Patient Panels at least monthly or more often if requested by Participant and agreed upon by Contexture. If a Health Plan Participant or its Business Associate fails to update their Patient Panel at least monthly, then Contexture has the right to discontinue the delivery of applicable Data services until a delta file with updates is delivered and processed.
4. Health Care Providers and Business Associates are responsible for notifying Contexture of changes to their Patient Panel via the provision of a delta file or other mutually agreeable alternative method. When a Provider no longer has a HIPAA-compliant reason for it or its Business Associate to receive Data for an individual, the Provider or Business Associate must notify Contexture as soon as possible by providing an updated delta file but in no case any less frequently than annually.

7.6 **HL7 Object Identifier (OID) Requirements**

To ensure effective Data management and secure interfacing between the HIE System and Participant's EHR systems, all Data Providers shall have a registered Participant Root OID issued by HL7.org. The OID must be unique and different from the electronic health record issued OID. The Participant must follow HL7 standards regarding OID branching. Participants with HL7 interfaces shall provide advance notice to Contexture of OID and facility (i.e., MSH:4) modifications to MSH:4 values.

7.7 **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.

7.8 **Asset and Configuration Management**

Contexture and its System Providers shall maintain an inventory of Contexture 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.

7.9 **Backups, Disaster Preparedness, and Emergency Management**

Contexture 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 Contexture System.

7.10 **Capacity Monitoring**

Contexture 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.

7.11 **System Monitoring and Operations**

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

7.12 **System and Services Acquisition**

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

7.13 **Technical Support for Participants**

Contexture 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.

7.14 **Contexture System Downtime, Maintenance, Updates, and Enhancements**

For the Contexture System to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that the Contexture 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 Contexture 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 **Contexture'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 Contexture 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.

8. NO INFORMATION BLOCKING POLICY

8.1 **Purpose**

The purpose of this policy is to support Contexture's and Participants' commitment to facilitating the timely access, exchange and use of EHI in compliance with Applicable Law.

8.2 **Scope**

This policy applies to Contexture and Participant Actors.

8.3 **Compliance with the Information Blocking Rule**

Contexture and its Participants will comply with Applicable Law in connection with HIE services, including the requirements of the Information Blocking Rule (if 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 for a Safe Harbor.

Contexture and Participant Actors may not engage in any practices that violate the Information Blocking Rule in connection with HIE services. This policy does not prevent Contexture or Participant Actors from engaging in practices that are Required by Law or that fall within a Safe Harbor. Contexture and Participant Actors 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 a Safe Harbor.

8.4 **Safe Harbors**

For illustrative and educational purposes only, below is a descriptive summary of the Safe Harbors set forth in the Information Blocking Rule. All of the regulatory conditions must be met in order for a Safe Harbor to apply. This policy does NOT provide a comprehensive explanation of all the Safe Harbor conditions or guidance regarding what Actors must do to qualify for a Safe Harbor.

8.4.1 **Preventing Harm**

The Preventing Harm Safe Harbor may apply when an Actor reasonably believes that a practice would substantially reduce a regulatory cognizable risk of harm to a natural person that otherwise would arise from the access, exchange or use of EHI, so long as the practice is no broader than necessary to reduce the risk of harm and all the regulatory conditions are met.

8.4.2 **Privacy**

The Privacy Safe Harbor may apply if an Actor does not fulfill a request to access, exchange or use EHI in order to protect an individual's right to confidentiality of EHI or privacy preferences, so long as the regulatory conditions of the applicable sub-exceptions within the Privacy Safe Harbor are met.

8.4.3 **Security**

The Security Safe Harbor may apply to practices that are directly related and tailored to safeguarding the confidentiality, integrity, and availability of EHI, so long as the regulatory conditions are met.

8.4.4 **Content and Manner**

An Actor will not violate the Information Blocking Rule if an Actor fulfills a request for access, exchange or use of EHI in the manner it is requested or in an alternative manner, so long as all the regulatory conditions are met (including compliance with the requirements of the Fees Safe Harbor

and Licensing Safe Harbor, if applicable). If fulfilling the request, even in an alternative manner, would impose a significant burden on the Actor, the Actor may seek to deny the request in compliance with the Infeasibility Safe Harbor.

8.4.5 **Infeasibility**

The Infeasibility Safe Harbor may apply in those circumstances where legitimate practical challenges may limit or prevent an Actor from complying with a request for access, exchange or use of EHI because of an uncontrollable event (such as a public health emergency), lack of technical capabilities (such as the ability to segment sensitive health information), legal rights, or other means necessary to fulfill the request, so long as the regulatory conditions are met.

8.4.6 **Fees**

An Actor will not violate the Information Blocking Rule by charging reasonable fees related to developing the technology and services giving access to the EHI, so long as the regulatory conditions are met.

8.4.7 **Licensing**

An Actor will not violate the Information Blocking Rule by licensing its technology and/or services used to access, exchange, or use EHI, so long as the regulatory conditions are met.

8.4.8 **Health IT Performance**

The Health IT Performance Safe Harbor is intended to apply to those practices that make health IT temporarily unavailable or degrade performance for the benefit and health of the overall performance of the health IT, so long as the regulatory conditions are met.

8.5 **Information Blocking Complaints**

8.5.1 Participants that reasonably believe Contexture or a Participant Actor is violating the Information Blocking Rule in connection with the HIE Services should promptly notify Contexture. Complaints may be submitted anonymously.

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

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

8.6 **Compliance**

Contexture management will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment or HIE participation. Where illegal activities are suspected, Contexture may report such activities to applicable authorities.