Arizona Health Information Exchange (HIE) Participant Policy Manual

Last updated

September 26, 2023

Contents

Definitions Policy **8**

Data Submission Policy **14**

Purpose 14

Scope 14

Definitions 14

Policy 14

Acceptable Data Formats 14

Prohibited Data Submissions 15

Requirements for Protected Data Submissions 15

Part 2 Data Submissions 15

HIPAA-Restricted Self-Pay Data 16

Requirements for Patient Panels and Member File Submissions 16

HL7 Object Identifier (OID) Requirements 17

Compliance 17

Who Should Read This Policy? 17

Reference/Citation 17

Cross-Reference 17

Revision Table 17

HIE Notice and Opt-Out Policy **19**

Purpose 19

Scope 19

Definitions 19

Policy 19

The HIE Notice 19

Health Current Responsibilities 19

Healthcare Provider Participant Responsibilities 19

The Opt-Out Right and Implementation 20
Opt-Out Requirements 20
Opt-Back-In Requirements 21
Compliance 21
Who Should Read This Policy? 21
Reference/Citation 21
Cross-Reference 21
Revision Table 22
Permitted Use Policy 23
Purpose 23
Scope 23
Definitions 23
Policy 24
Limitations on the Permitted Use Cases Required by Applicable Law 24
Individuals with an Opt-Out Status 24
Minimum Necessary Standard 24
Part 2 Data Access 24
Other Trusted Exchange Requirements 25
Financial Information from Claims Data 25
Health Care Provider Permitted Use Cases and Requirements 25
Treatment, Payment and Limited Health Care Operations 25
Individuals for Whom Data May Be Accessed 26
Minimum Necessary Standard 26
Health Plan Permitted Use Cases and Requirements 26
Payment and Limited Healthcare Operations 26
Individuals for Whom Data May Be Accessed 27
Minimum Necessary Standard 27

Public Health Authority Permitted Use Cases and Requirements 27
Limited Public Health Activities 27
Individuals for Whom Data May Be Accessed 27
Minimum Necessary Standard 27
Medical Examiner Permitted Use Cases and Requirements 27
Medical Examiner Activities 27
Individuals for Whom Data May Be Accessed 28
Minimum Necessary Standard 28
Organ Procurement Permitted Use Cases and Requirements 28
Organ Procurement 28
Individuals for Whom Data May Be Accessed 28
Minimum Necessary Standard 28
Health Current Permitted Use Cases and Requirements 28
Health Current Permitted Uses 28
Minimum Necessary Standard 29
Process for Approval of New Use Cases 29
Compliance 29
Who Should Read This Policy? 30
Reference/Citation 30
Cross-Reference 30
Revision Table 30
Minimum Necessary Standard Procedure 31
Purpose 31
Scope 31
Definitions 31
Policy 32
Participant and Business Associate Uses, Disclosures or Requests of Data 32

Health Current's Uses, Disclosures or Requests of Data 32
Internal Uses 32
Routine Disclosures or Requests 32
Reasonable Reliance 33
Nonroutine Disclosures or Requests 33
Entire Medical Record 34
Compliance 34
Who Should Read This Policy? 34
Reference/Citation 34
Cross-Reference 34
Revision Table 34
No Information Blocking Policy 35
Purpose 35
Scope 35
Definitions 35
Policy 36
Compliance with the Information Blocking Rule 36
Safe Harbors 36
Preventing Harm 36
Privacy 37
Security 37
Content and Manner 37
Infeasibility 37
Fees 37
Licensing 37
Health IT Performance 37
Information Blocking Complaints 38

Compliance 38
Who Should Read This Policy? 38
Reference/Citation 38
Cross-Reference 38
Revision Table 38
Individual Rights Policy 39
Purpose 39
Scope 39
Definitions 39
Policy 39
Individual Access Requests 39
Participant Responsibilities 40
All Participants 40
Data Suppliers (except for Part 2 Program Data Suppliers) 40
Part 2 Program Data Supplier Responsibilities 42
Health Current Responsibilities 42
Individual Amendment Requests 43
Individual Accounting Requests 43
Participant Responsibilities 43
Health Current Responsibilities 43
Compliance 43
Who Should Read This Policy? 43
Reference/Citation 44
Cross-Reference 44
Revision Table 44
HIE Security and Maintenance Policy 45
Purpose 45

Scope 45
Definitions 45
Policy 45
Security Procedures 45
HIE Downtime, Maintenance and Updates 46
Compliance 46
Who Should Read This Policy? 46
Reference/Citation 46
Cross-Reference 46
Revision Table 47

DEFINITIONS POLICY

Document Name:	Definitions Policy				
Document Code:	POL-ADM-0020-A			**Formerly:** (if applicable)	See below
Approval Authority:	Board of Directors	**Adopted:**	1/26/2021	**Reviewed: Frequency:**	Annually
Responsible Executive:	Melissa Kotrys	**Revised:**	See below		
Responsible Office:	Administration	**Contact:**	Melissa Kotrys		
Distribution:	**X** - Staff | **X**- Participants **X** – Vendors | **X** - Public	Posted Locations:	**X** - Internal Policy Library **X** - Public Website		

1. **Purpose**
   To provide a single reference for defined terms in the HIE Participant Policy Manual (Manual). Unless otherwise defined in a specific policy, all capitalized terms in this Manual will have the same meaning as provided below or elsewhere in this Manual, in the Health Current Participation Agreement or HIPAA, all as amended from time to time.

2. **Scope**
   This policy applies to all documents in the HIE Participant Policy Manual.

3. **Definitions**
   See Definitions Policy.

4. **Policy**

   4.1. **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.

   4.2. **Applicable Law** means federal, state, and local statutes and regulations that are applicable to Health Current, Participants, Authorized Recipients, or other individuals who access Data through the HIE.

   4.3. **Authorized Recipient(s)** means a person or entity that has a HIPAA Authorization to access Data of the individual who is the subject of the HIPAA Authorization for the purposes given in the HIPAA Authorization.

4.4. **Claims Data** means those standard transactions between two parties to carry out financial or administrative activities related to healthcare, including bills sent by healthcare providers to a health plan to request payment for medical services and payment of such bills by a health plan. Claims Data consists of two components: (1) clinical data; and (2) financial data. For purposes of the Permitted Use Policy, the restrictions on Claims Data apply to the financial data component only and are necessary for compliance with Applicable Law, such as antitrust laws.

4.5. **Data** means any individually identifiable information transmitted to Health Current by Data Suppliers 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 Health Current to distinguish between Data that is and is not PHI. Thus, for purposes of this HIE Participant Policy Manual all Data accessible through the HIE is treated as PHI.

4.6. **Data Supplier** means an entity that makes Data available for access through the HIE and has entered into a Participation Agreement.

4.7. **De-identified Data** means Data that complies with the HIPAA de-identification standards at 45 C.F.R. § 164.514.

4.8. **DOJ** means the United States Department of Justice.

4.9. **FTC** means the Federal Trade Commission.

4.10. **Healthcare Provider**, within the scope of its HIPAA definition, includes hospitals, physicians and physician practices, behavioral health clinics, clinical laboratories, nursing homes, ambulatory surgical centers, home health agencies, hospice programs, outpatient rehabilitation facilities, imaging facilities, and pharmacies. Health Current may determine that other types of entities or persons meet the definition of a Healthcare Provider. Please note that for purposes of the No Information Blocking Policy, only Healthcare Providers who fall within one of the enumerated categories set forth in in 42 U.S.C. § 300jj(3) will constitute an Actor subject to the Information Blocking Rule.

4.11. **Health Current Workforce Members** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Health Current, is under the direct control of Health Current.

4.12. **Health Plan**, within the scope of its HIPAA definition, includes health insurance companies regulated by the Arizona Department of Insurance (ADOI), health maintenance organizations (HMOs), Medicaid (AHCCCS) plans, and group health plans that are offered to individuals through their employers. Health Current may determine that other types of entities meet the definition of a health plan.

4.13. **HHS** means the United States Department of Health and Human Services.

4.14. **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, the term HIE has the meaning set forth in 45 C.F.R. § 171.102. The HIE is distinguishable from Health Current's other business lines, including without limitation CommunityCares and Arizona Healthcare Directives Registry (AzHDR).

4.15. **HIPAA** collectively refers to the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and their implementing regulations (see 45 C.F.R. Parts 160, 162, and 164), all as amended from time to time.

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

4.17. **HIPAA-Restricted Self-Pay Data** means Data pertaining to a healthcare item or service for which an individual has fully paid for out-of-pocket and which the patient requested not to be disclosed to a health plan.

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

4.19. **Insurance Companies** means entities (other than Health Plans) that offer insurance products, such as life insurance, disability, and long-term care insurance.

4.20. **Limited Healthcare Operations** means those 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).

4.21. **Limited Public Health Activity** means a Public Health Authority that is authorized by law to collect or receive Data for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority, see 45 C.F.R. § 164.512(b)(1)(i). Limited Public Health Activities do **NOT** include fraud and abuse detection activities, provider or facility monitoring, or other health oversight activities or law enforcement activities.

4.22. **Master Person Index or MPI** means the database(s) comprised of individual identifiers, including a unique index identifier, that is used to identify and match individuals across databases and systems.

4.23. **Medical Examiner** means a person or entity authorized by law to identify a deceased person, determine a cause of death of a deceased individual, or perform other duties as authorized by law, see A.R.S. § 11-591 et seq.

4.24. **Organ Procurement Organization** means any organization that is engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purposes of facilitating organ, eye or tissue donation and transplantation, which may include (i) any organization designated by the Secretary of the United States Department of Health and Human Services as an organ procurement organization, (ii) a tissue bank, or (iii) eye bank, see A.R.S. § 36-841.

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

4.26. **Part 2 Consent Form** means a form approved by Health Current for accessing Part 2 Data through the HIE and that meets Part 2's consent requirements.

4.27. **Part 2 Data** means information subject to and protected by Part 2.

4.28. **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.

4.29. **Participant** means a person or legal entity that has signed a Participation Agreement.

4.30. **Participation Agreement** means the written agreement—including all amendments, addendum, attachments, exhibits, or statements of work thereto—that a Participant enters into with Health Current that defines such Participant's obligations and responsibilities related to disclosing, accessing, exchanging and using Data through the HIE.

4.31. **Payment** means activities defined by HIPAA, including but not limited to activities undertaken by:

4.31.1. A health plan to obtain premiums and/or to determine or fulfill coverage obligations and provisions of benefits under a health plan; and

4.31.2. A Healthcare Provider or health plan to obtain or provide reimbursement for the provision of healthcare.

Payment does **NOT** include activities defined as Healthcare Operations at 45 C.F.R. § 164.501, such as underwriting or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits.

4.32. **Permitted Use** means the specific reasons for which Participants may access Data through the HIE, and for which Health Current may use and disclose Data in connection with the HIE. Please see the Permitted Use Policy.

4.33. **Psychotherapy Notes**, as defined by HIPAA, means notes recorded (in any medium) by a healthcare provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy Notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis; functional status; the treatment plan; symptoms; prognosis; and progress to date.

4.34. **Public Health Authority** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

4.35. **Treatment**, as defined by HIPAA, means the provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a healthcare provider with a third party; consultation between healthcare providers relating to a patient; or the referral of a patient for healthcare from one healthcare provider to another.

5. Compliance

Health Current 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, Health Current may report such activities to applicable authorities.

6. Who Should Read this Policy?

6.1. Health Current HIE Participants
6.2. Health Current Staff
6.3. Health Current HIE Subcontractors

7. Reference/Citation

Embedded.

8. Cross Reference and/or Attachments

9. Revision Table

Version	Date	Description of Change	Revised By
B	6/15/2022	Update to add definition of MPI and expand definition of Limited Public Health Activity	Approved by Policy Advisory Council on June 15, 2022; Approved by Contexture Board of Directors on July 26, 2022.
A	1/26/2021	Initial Release	Board of Directors

DATA SUBMISSION POLICY

Document Name:	Data Submission Policy				
Document Code:	POL-ADM-0021-A			**Formerly:** (if applicable)	See below
Approval Authority:	Board of Directors	**Adopted:**	1/26/2021	**Reviewed: Frequency:**	Annually
Responsible Executive:	Melissa Kotrys	**Revised:**	See below		
Responsible Office:	Administration	**Contact:**	Melissa Kotrys		
Distribution:	**X** - Staff | **X-** Participants **X** – Vendors | **X** - Public	**Posted Locations:**	**X -** Internal Policy Library **X -** Public Website		

1. Purpose

To help ensure that Data made accessible by Data Suppliers through the HIE is accessible in accordance with Applicable Law, including laws that are more stringent than HIPAA with respect to certain types of Data.

2. Scope

This policy applies to Participants that are Data Suppliers and, where specifically stated, to Participants (or their designated Business Associates) that submit patient panels or member files to Health Current for attributed patients or members as required for the receipt of HIE Services, including Alerts or other patient-based notifications

3. Definitions

See Definitions Policy.

4. Policy

4.1. Acceptable Data Formats

Data Suppliers must provide access to Data using content and manner standards that are supported by the HIE. This is necessary to ensure that the Data supplied can be accessed, exchanged, and used by Participants for Permitted Uses. Health Current can accept and support Data in the following formats:

4.1.1. HL7 V2
4.1.2. HL7 V3 (XML/CCD)
4.1.3. Claim and Claim Line Feed (CCLF) (Claims Data only)
4.1.4. EDI/X12 (Claims Data only)
4.1.5. Flat file formats (e.g., comma delimited)

Technology is constantly changing and improving. Health Current may accept and support other Data formats in accordance with nationally recognized standards for HIE. Data

Suppliers may consult, as needed, with their Health Current Account Manager to determine whether other content and manner standards may be accepted and supported by the HIE.

4.2. Prohibited Data Submissions

Applicable Law limits the circumstances under which certain types of Data may be disclosed to Health Current and/or accessed and exchanged with other Participants through the HIE. Because of these legal restrictions, and technical and operational complexities, it is not feasible for Health Current to support the exchange of certain types of Data. Thus, Participants must NOT submit the following types of Data to the HIE in any form:

4.2.1. Psychotherapy Notes (as defined by HIPAA);

4.2.2. Immunization information of minor children where the parent has provided Participant with a form that prohibits disclosure of the immunization information under A.R.S. § 36-135(I); and

4.2.3. Any other Data that Participant is not permitted by Applicable Law to disclose to Health Current and/or to make accessible to other Participants for Permitted Uses. For example, if a Participant chooses to grant an individual's request to restrict the use of the individual's Data for HIPAA-permitted Treatment, Payment and Limited Healthcare Operations purposes (other than HIPAA-Restricted Self-Pay Data) or other Permitted Uses, Participant must not make this restricted Data accessible through the HIE because the technical and administrative processes necessary to honor the privacy restrictions are not currently available.

4.3. Requirements for Protected Data Submissions

4.3.1. Part 2 Data Submissions

Federal law gives greater privacy protections to Part 2 Data. Health Current must segregate Part 2 Data to comply with these more restrictive requirements. Due to current technical limitations and medical record keeping practices, it is often not feasible to separate Part 2 Data from other Data supplied by Part 2 Programs. Health Current thus segregates all Data from Data Suppliers that operate Part 2 Programs from other Data accessible through the HIE unless the Data Supplier can segment the Part 2 Data from the other Data appropriately.

Before submitting any Data to the HIE, Data Suppliers must notify their designated Health Current Account Manager in writing if they operate a Part 2 Program so that Health Current can properly segregate the Data.

Data Suppliers that are not Part 2 Programs, but are in possession of Part 2 Data, must **NOT** disclose the Part 2 Data to Health Current, unless they have (1) a mechanism to segregate the Part 2 Data from other Data, and (2) Health Current's advance written consent to supply the Part 2 Data to the HIE. This is necessary for Health Current to determine whether the appropriate legal, technical, and administrative processes are available and in place to facilitate the sharing of Part 2 Data held by non-Part 2 Programs in compliance with Part 2.

4.3.2. HIPAA-Restricted Self-Pay Data

HIPAA gives individuals the right to ask their healthcare providers not to disclose protected health information (PHI) to health plans, where individuals have paid for healthcare services in full out-of-pocket and the PHI relates to those healthcare services. HIPAA requires healthcare providers to honor such requests. For Data Suppliers and Health Current to comply with such restrictions, the Data Supplier must either:

4.3.2.1. Not make the HIPAA-Restricted Self-Pay Data accessible through the HIE; or

4.3.2.2. Notify Health Current of the HIPAA-Restricted Self-Pay Data. The Data Supplier must notify Health Current of HIPAA-Restricted Self-Pay Data at the time of submission to the Health Current. If an individual designates Data as HIPAA-Restricted Self-Pay Data after the Data Supplier has supplied that Data to Health Current, Data Supplier must promptly notify Health Current of the new designation. Data Suppliers must cooperate with Health Current on the technical and administrative process the Data Supplier will use to notify Health Current and to segment the HIPAA-Restricted Self-Pay Data from other Data.

4.4. Requirements for Patient Panel and Member File Submissions

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

4.4.1 All Participants must submit Patient Panels that comply with Health Current's standard Patient Panel specifications, which are supplied during the HIE onboarding process. By including an Individual on Participant's Patient Panel, Participant represents that it has a current HIPAA-compliant Treatment, Payment or Limited Healthcare Operations relationship with the Individual.

4.4.2 After the submission of an initial Patient Panel, all Participants 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 Health Current 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 Health Current to submit updates to a Patient Panel via an alternative method.

4.4.3 **Health Plans:** Health Plans must update their Patient Panels at least monthly or more often if requested by Participant and agreed upon by Health Current. If a Health Plan Participant fails to update their Patient Panel at least monthly, then Health Current has the right to discontinue the delivery of applicable Data services until a delta file with updates is delivered and processed.

4.4.4 **Providers:** Providers are responsible for notifying Health Current of changes to their Patient Panel via the provision of a delta file or other mutually agreeable alternative method. When Provider no longer has a HIPAA-compliant reason to receive Data for an Individual, Provider must notify Health Current as soon as possible by providing an updated delta file but in no case any less frequently than annually.

4.5. HL7 Object Identifier (OID) Requirements

To ensure effective Data management and secure interfacing between the HIE System and Participant's EHR systems, all Data Suppliers 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.

5. Compliance

Health Current 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, Health Current may report such activities to applicable authorities.

6. Who Should Read this Policy?

6.1. Health Current HIE Participants
6.2. Health Current Staff
6.3. Health Current HIE Subcontractors

7. Reference/Citation

8. Cross Reference and/or Attachments

9. Revision Table

Version	Date	Description of Change	Revised By
C	9/26/2023	Update to Include Object Identifier Requirements	Contexture Approved by Policy Advisory Committee on 9/7/2023 Approved by BOD on 9/26/2023
B	9/27/2022	Update to Include Patient Panel Requirements	Approved by Policy Advisory Committee on 9/7/2022

			Approved by BoD on 9/27/2022
A	1/26/2021	Initial Release	Board of Directors

HIE NOTICE AND OPT OUT POLICY

Document Name:	HIE Notice and Opt Out Policy				
Document Code:	POL-ADM-0022-A			**Formerly:** (if applicable)	See below
Approval Authority:	Board of Directors	**Adopted:**	1/22/2019	**Reviewed: Frequency:**	Annually
Responsible Executive:	Melissa Kotrys	**Revised:**	See below		
Responsible Office:	Administration	**Contact:**	Melissa Kotrys		
Distribution:	**X** - Staff | X-Participants **X** – Vendors | X - Public	**Posted Locations:**	**X** - Internal Policy Library **X** - Public Website		

1. **Purpose**
   This policy explains how Health Current and Participants will work together to ensure that individuals have the information necessary to make a meaningful choice regarding whether their Data is accessible through the HIE, as well as the process for implementing an individual's opt out right.

2. **Scope**
   This policy applies to Health Current and Healthcare Provider HIE Participants.

3. **Definitions**
   See Definitions Policy.

4. **Policy**

   4.1. The HIE Notice

   Arizona's Health Information Organization Law (A.R.S. §§ 36-3801 through -3809) requires Healthcare Providers to give individuals notice of their HIE participation and the opportunity to opt out of having their Data made accessible through the HIE.

   4.2. Health Current Responsibilities

   Health Current is required to maintain a notice of health information practices (the "HIE Notice"). Health Current will post its current HIE Notice conspicuously on its website. Health Current will also provide an individual with a copy of the HIE Notice within thirty (30) calendar days after Health Current receives a written request for that information from the individual.

   4.3. Healthcare Provider Participant Responsibilities

   Healthcare Provider Participants must distribute the HIE Notice and document its distribution as required by Arizona's Health Information Organization law, see A.R.S. § 36-

3804. Specifically, a Healthcare Provider is required to distribute the HIE Notice under the following circumstances:

4.3.1. The Healthcare Provider (or its Business Associate) makes Data generated or maintained by the Healthcare Provider accessible through the HIE; or

4.3.2. The Healthcare Provider Accesses Data directly through the HIE.

A Healthcare Provider that only indirectly receives Data that originated from the HIE through an accountable care organization (ACO), clinically integrated network (CIN), Health Plan or similar organization (collectively, an "**Intermediary Organization**") is not required to distribute the HIE Notice. However, a Healthcare Provider who makes its Data accessible through the HIE indirectly through an Intermediary Organization must distribute the HIE Notice.

4.4. The Opt Out Right Implementation

Except as otherwise provided in state or federal law, an individual may choose not to allow his or her Data to be accessible through the HIE. Any individual may download the most current version of the Health Current Opt Out Form from Health Current's website. If an individual chooses to opt out, the individual must complete the Health Current Opt Out Form and return it to any Healthcare Provider Participant.

An individual may choose to opt back in at any time. To opt back in, the individual must either: (1) complete a Health Current Opt-Back-In Form and return it to a Healthcare Provider Participant; or (2) otherwise indicate in writing an intent to opt back in, such as by signing an authorization or consent to disclose individually identifiable health information through the HIE.

Participants will maintain documentation of these completed forms for at least six (6) years.

4.5. Opt Out Requirements

4.5.1. Participant Responsibilities

Participants will honor an individual's choice to opt out of HIE participation. However, Participants must not improperly encourage or induce an individual to opt out.

A Healthcare Provider Participant who receives an individual's completed Health Current Opt Out Form must promptly notify Health Current of the individual's decision to opt out of the HIE. A Healthcare Provider Participant must notify Health Current within fifteen (15) calendar days of the Healthcare Provider Participant's receipt of the Health Current Opt Out Form from the individual.

A Healthcare Provider Participant must notify Health Current using the following methods:

4.5.1.1. Completing the bottom section of the Health Current Opt Out Form and securely faxing it to Health Current; or

4.5.1.2. Utilizing a mutually agreed upon method for capturing the individual's opt-out decision electronically and transmitting that decision to Health Current.

4.5.2. Health Current Responsibilities

Health Current will assign an opt out status to an individual within thirty (30) calendar days of receiving the individual's opt out decision from a Healthcare Provider Participant. If an individual chooses to opt out, his or her Data will not be accessible through the HIE, even in the event of a medical emergency. An individual's opt out status will not affect a Participant's or Health Current's use or disclosure of Data through means other than the HIE. Nor will it prohibit Health Current from disclosing Data as required by law, such as obligations to perform mandatory public health reporting.

4.6. Opt Back In Requirements

4.6.1. Participant Responsibilities

A Healthcare Provider Participant will promptly notify Health Current of an individual's opt back in decision. A Healthcare Provider Participant must notify Health Current within fifteen (15) calendar days of the Healthcare Provider Participant's receipt of the Health Current Opt-Back-In Form. A Healthcare Provider Participant must notify Health Current using the same secure fax or other mutually agreed upon electronic method of transmission described above for implementing an individual's opt out right.

4.6.2. Health Current Responsibilities

Health Current will implement an individual's opt-back-in decision within thirty (30) calendar days of Health Current receiving a completed Health Current Opt-Back-In Form.

5. Compliance

Health Current 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, Health Current may report such activities to applicable authorities.

6. Who Should Read this Policy?

6.1. Health Current HIE Participants
6.2. Health Current Staff
6.3. Health Current HIE Subcontractors

7. Reference/Citation

Embedded.

8. Cross Reference and/or Attachments

9. Revision Table

Version	Date	Description of Change	Revised By
A	1/26/2021	Initial Release	Board of Directors

PERMITTED USE POLICY

Document Name:	Permitted Use Policy				
Document Code:	POL-ADM-0023-A			**Formerly:** (if applicable)	See below
Approval Authority:	Board of Directors	**Adopted:**	Jan 1, 2021	**Reviewed: Frequency:**	Annually
Responsible Executive:	Melissa Kotrys	**Revised:**	See below		
Responsible Office:	Administration	**Contact:**	Melissa Kotrys		
Distribution:	**X** - Staff | **X-** Participants **X** – Vendors | **X** - Public	**Posted Locations:**	**X** - Internal Policy Library **X** - Public Website		

1. **Purpose**
   This policy describes the specific purposes for which Participants may access Data through the HIE in accordance with Applicable Law and within the technical and operational framework that Health Current and its Participants can reasonably support. It also explains how Health Current may use and disclose Data in connection with the HIE.

2. **Scope**
   This policy applies to Health Current and its Participants. Due to legal, technical and operational limitations, access to the HIE is currently limited to Participants that are:
   2.1 Health Care Providers and their designated Business Associates;
   2.2 Health Plans and their designated Business Associates;
   2.3 Public Health Authorities;
   2.4 Medical Examiners; and
   2.5 Organ Procurement Organizations.
   Each type of Participant may only access Data for the Permitted Uses that apply to them. Health Current may also use and disclose Data for the Permitted Uses set forth in this policy.

   Once Data from the Health Current 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.

3. **Definitions**
   See Definitions Policy.

4. Policy

4.1. Limitations on the Permitted Use Cases Required by Applicable Law

Complex state and federal health information privacy laws may apply to some or all the Data accessible through the HIE. Accordingly, Health Current and its Participants must satisfy certain legally required preconditions and/or honor legally required limitations or requirements on their access and exchange of Data through the HIE. **Participants must observe the limitations covered in this Section in connection with their access of Data for Permitted Uses.**

4.1.1. Individuals with an Opt Out Status

As explained in the HIE Notice and Opt Out Policy, individuals have a right to opt out of having their Data made accessible through the HIE, except as otherwise provided in state or federal law. Accordingly, Participants may not access Data of individuals who have opted out for the Permitted Uses listed in this policy, unless access is required by law.

In its capacity as a Business Associate of Data Suppliers, Health Current may receive and maintain Data on individuals who have exercised their opt out right. Health Current and Participants collectively will implement the necessary technical and administrative processes to honor an individual's documented opt out request in accordance with Health Current's HIE Notice and Opt Out Policy.

4.1.2. Minimum Necessary Standard

The HIPAA minimum necessary standard may apply to certain Permitted Uses, as required by HIPAA. Health Current and Participants must comply with procedures approved by the Health Current Data Governance Council or the Board of Directors to implement the HIPAA minimum necessary standard.

4.1.3. Part 2 Data Access

Part 2 gives heightened privacy protections to Part 2 Data (certain kinds of substance use disorder information). As explained in the Data Submission Policy, Health Current keeps all Data from Part 2 Programs segregated from other Data in the HIE and protects it in accordance with Part 2 due to current technical and administrative limitations on the ability to segment Part 2 Data from other Data.

Participant may access Part 2 Data under the following circumstances:

4.1.3.1. Part 2 Consent Form

Participants may access Part 2 Data through the HIE pursuant to a Part 2 Consent Form. Health Current requires use of its approved Part 2 Consent Form because this is the only feasible option available to Health Current 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 Health Current's technical and administrative processes related to documenting consent.

4.1.3.2. Medical Emergency Access

Healthcare Provider Participants may access Part 2 Data through the HIE for emergency Treatment purposes, but only to the extent necessary to meet a bona fide medical emergency in which the individual's prior consent cannot be obtained.

4.1.3.3. Case-by-Case Determinations

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

4.1.4. Other Trusted Exchange Requirements

Health Current participates in multi-party trust arrangements with other HIEs, federal agencies, and other entities and organizations that desire to engage in electronic health information exchange for purposes permitted by Applicable Law ("Trusted HIE Connections"). Participation in Trusted HIE Connections promotes interoperability by facilitating secure access to health information when and where it is needed to support patient care, Healthcare Operations, and public health activities. For example, Health Current participates in eHealth Exchange—a data sharing network of governmental and non-governmental exchange partners that share information for specific purposes—and Patient Centered Data Home (PCDH) networks—a data sharing network of HIEs that desire to send electronic notifications to members of an individual's care team that reside in different geographic jurisdictions. When accessing Data through a Trusted HIE Connection, Participant must comply with any requirements applicable to that Trusted HIE Connection, such as limitations on the purposes for which Data may be accessed through the Trusted HIE Connections.

4.1.5. Financial Information from Claims Data

If the Claims Data supplied to Health Current includes financial information, Health Current will restrict Participant access to the financial component of Claims Data of other Data Suppliers consistent with federal antitrust policy established by the DOJ and FTC in the Statements of Antitrust Enforcement Policy in Healthcare (Aug. 1996), as amended from time to time.

4.2. Healthcare Provider Permitted Use Cases and Requirements

4.2.1. Treatment, Payment and Limited Healthcare Operations

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

4.2.1.1. Treatment (including care coordination, case management and transition of care planning);

4.2.1.2. Payment; and

4.2.1.3. Limited Healthcare Operations (including population health activities), so long as:

4.2.1.3.1. The Healthcare Provider has (or had) an established relationship with the individual who is the subject of the Data and the Data pertains to that relationship; and

4.2.1.3.2. The Healthcare Provider is a HIPAA Covered Entity.

4.2.2. Individuals for Whom Data May Be Accessed

4.2.2.1. Treatment and Payment

Access is permitted for permitted for Data of individuals who are:

4.2.2.1.1. Current patients of the Healthcare Provider;

4.2.2.1.2. Prospective patients with whom the Healthcare Provider is expected to establish a treatment relationship (for example, an individual who is scheduled for an upcoming appointment or who has been assigned to the Healthcare Provider by a Health Plan); and

4.2.2.1.3. Past patients for whom the Healthcare Provider is transitioning to a new Healthcare Provider (for example, individuals who have an outstanding payment obligation to the Healthcare Provider that is transitioning care).

4.2.2.2. Limited Healthcare Operations

Access is permitted for Data of individuals who are current or past patients of the Healthcare Provider.

4.2.3. Minimum Necessary Standard

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 Data requests to only the Data needed for the Healthcare Provider to conduct the Payment or Limited Healthcare Operations activities. Specifically:

4.2.3.1. The request for Data for Payment purposes should not exceed Data generated during the thirteen (13) months prior to the request.

4.2.3.2. The request for Data for Limited Healthcare Operations activities should not exceed Data generated during the thirty-six (36) months prior to the request.

4.3. Health Plan Permitted Use Cases and Requirements

4.3.1. Payment and Limited Healthcare Operations

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

4.3.1.1. Payment; and

4.3.1.2. Limited Healthcare Operations (including care coordination, case management, transition of care planning, and population health activities), so long as:

4.3.1.2.1 The Health Plan has (or had) an established relationship with the individual who is the subject of the Data and the Data pertains to that relationship; and

4.3.1.2.2 The Health Plan is a HIPAA Covered Entity.

4.3.2. Individuals for Whom Data May Be Accessed

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.

4.3.3. Minimum Necessary Standard

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. Specifically:

4.3.3.1. The request for Data for Payment purposes should not exceed Data generated during the thirteen (13) months prior to the request.

4.3.3.2. The request for Data for Limited Healthcare Operations activities should not exceed Data generated during the thirty-six (36) months prior to the request.

4.4. Public Health Authority Permitted Use Cases and Requirements

4.4.1. Limited Public Health Activities

A Public Health Authority that is a Participant may access Data for a Limited Public Health Activity. This use case is conditioned on there being adequate technical and/or administrative procedures in place to provide access in compliance with Applicable Law. Health Current will not give a Public Health Authority direct access to the HIE for a Limited Public Health Activity until this legal precondition is satisfied.

4.4.2. Individuals for Whom Data May Be Accessed

Access is permitted for Data of individuals who are the subject of a Limited Public Health Activity.

4.4.3. Minimum Necessary Standard

The HIPAA minimum necessary standard applies to the Limited 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 particular Limited Public Health Activity.

4.5. Medical Examiner Permitted Use Cases and Requirements

4.5.1. Medical Examiner Activities

A Medical Examiner that is a Participant may access Data for purposes of identifying a deceased person, determining a cause of death, conducting a death investigation, or performing other duties as authorized by Applicable Law, see A.R.S. § 11-594 (collectively, **"Medical Examiner Activities"**).

4.5.2. Individuals for Whom Data May Be Accessed

Access is permitted for Data of individuals who are the subject of the Medical Examiner Activities.

4.5.3. Minimum Necessary Standard

The HIPAA minimum necessary standard applies to the Medical Examiner Activities use case. To comply with the minimum necessary standard, the Medical Examiner will limit its request to only the Data needed for the Medical Examiner Activity, and which was generated during the twenty-four (24) months prior to the request.

4.6. Organ Procurement Permitted Use Cases and Requirements

4.6.1. Organ Procurement

An Organ Procurement Organization that is a Participant may access Data for the purpose of facilitating organ, eye or tissue donation and transplantation as permitted by Applicable Law.

4.6.2. Individuals for Whom Data May Be Accessed

Access is permitted for Data of individuals who are donors or prospective donors of their organ(s), eye(s) or tissue(s).

4.6.3. Minimum Necessary Standard

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.

4.7. Health Current Permitted Use Cases and Requirements

4.7.1. Health Current Permitted Uses

Health Current is a Business Associate of its Participants. Health Current may not use or disclose Data in a manner prohibited by Applicable Law. Specifically, Health Current may access, use and disclose Data for the following Permitted Uses:

4.7.1.1. As required by law, including if required by a subpoena that satisfies the requirements of Applicable Law (see A.R.S. § 36-3808);
4.7.1.2. As necessary to perform services under the Participation Agreement and to assist Participants (and Participants' Business Associates) in the Permitted Uses;
4.7.1.3. As directed in writing by the Data Supplier(s) that provided the Data;
4.7.1.4. To provide access to an individual in accordance with A.R.S. § 36-3802 (see the Individual Rights Policy);
4.7.1.5. To provide access to Authorized Recipients, such as Insurance Companies, if Health Current has the necessary technical and administrative processes in place to support Authorized Recipients access in accordance with Applicable Law and healthcare industry standard security practices;
4.7.1.6. To conduct Limited Healthcare Operations on behalf of Covered Entities;
4.7.1.7. To conduct Limited Public Health Activities;

4.7.1.8. To facilitate health information exchange through Trusted HIE Connections for any of the Permitted Uses set forth in this policy, including (but not limited to) Treatment, Payment, Limited Healthcare Operations, and Limited Public Health Activities;

4.7.1.9. To create De-Identified Data to be used and disclosed for purposes permitted by Applicable Law (including, but not limited to, Research if applicable state law requirements are met, see A.R.S. § 36-3805); and

4.7.1.10. For Health Current's own management and administration (including but not limited to operation of its Master Person Index) or to carry out its legal responsibilities, including (but not limited to) audit, legal defense and liability, record keeping, and similar obligations.

4.7.2. Minimum Necessary Standard

Health Current will comply with its Minimum Necessary Standard Procedure with respect to the Health Current Permitted Use cases.

4.8. Process for Approval of New Use Cases

To make changes to this policy, the following process will be followed:

4.8.1. Health Current or any Participant may propose a new use case for consideration by the Health Current Data Governance Council. The proposal should set forth specific details regarding:

4.8.1.1. The purpose of the new use case;

4.8.1.2. Which category of Participants or Health Current is proposed to have access to Data under the new use case;

4.8.1.3. A description of the individuals for whom Data may be accessed;

4.8.1.4. The types of Data that may be accessed for the use case; and

4.8.1.5. The time for which Data may be accessed (e.g., "Data created during the 36 months prior to the request"), or other criteria to be used to implement the HIPAA minimum necessary standard.

4.8.2. The Health Current Data Governance Council will review new proposed use cases. The Council will issue a schedule for consideration of new use cases that will be made available to all Participants from time to time.

4.8.3. If the Health Current Data Governance Council recommends approval of a new use case, it will forward a completed "Permitted Use Approval" checklist along with its recommendation to the Board of Directors for consideration.

4.8.4. If a new use case is approved by the Board of Directors and is consistent with Applicable Law, this policy will be amended to reflect such new use case and notice will be provided to all Participants consistent with the Health Current Participation Agreement.

5. Compliance

Health Current 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, Health Current may report such activities to applicable authorities.

6. **Who Should Read this Policy?**
   - **6.1.** Health Current HIE Participants
   - **6.2.** Health Current Staff
   - **6.3.** Health Current HIE Subcontractors

7. **Reference/Citation**
   Embedded.

8. **Cross Reference**

9. **Revision Table**

Version	Date	Description of Change in Last 5 Years	Revised By
B	6/15/2022	Updated Permitted Use Policy to expressly authorize Health Current's use of HIE Data for MPI administration and for Limited Public Health Activity Use Cases. Approved by Policy Advisory Council on June 15, 2022; Approved by Contexture Board of Directors on July 26, 2022.	Contexture
A	1/26/2021	Initial Release	Board of Directors

MINIMUM NECESSARY STANDARD PROCEDURE

Document Name:	Minimum Necessary Standard Procedure				
Document Code:	POL-ADM-0024-A			**Formerly:** (if applicable)	See below
Approval Authority:	Board of Directors	**Adopted:**	1/31/2018	**Reviewed: Frequency:**	Annually
Responsible Executive:	Melissa Kotrys	**Revised:**	See below		
Responsible Office:	Administration	**Contact:**	See below		
Distribution:	**X** - Staff | **X**- Participants **X** – Vendors | **X** - Public	**Posted Locations:**	**X** - Internal Policy Library **X** - Public Website		

1. **Purpose**
   This procedure is intended to help ensure that Health Current and Participants (including Business Associates) use, request and disclose only the minimum amount of Data necessary for accomplishing the intended Permitted Use. This is necessary for compliance with the HIPAA minimum necessary standard, see 45 C.F.R. §§ 164.502(b) and 164.514(d). This procedure describes when the minimum necessary standard applies and how to satisfy its requirements.

2. **Scope**
   This procedure applies to Health Current and Participants (including Business Associates). This procedure does not apply to the following Permitted Uses of Data:
   - **2.1** Disclosures to or requests from Healthcare Providers for Treatment;
   - **2.2** Disclosures to the individual who is the subject of the Data;
   - **2.3** Disclosures made pursuant to a HIPAA Authorization;
   - **2.4** Disclosures required by law; and
   - **2.5** Uses or disclosures required for compliance with HIPAA, including to HHS for investigations or compliance audits.

   All other uses, disclosures and requests for Data are subject to the minimum necessary standard.

3. **Definitions**
   See Definitions Policy.

4. Policy

4.1. Participant and Business Associate Uses, Disclosures or Requests of Data

Participants and their Business Associates will comply with their own minimum necessary standard policies and procedures, as well as any other restrictions set forth in Health Current's Permitted Use Policy and this procedure, in connection with their use of HIE services.

If a Participant (or its Business Associate) wishes to access Data for a Permitted Use that exceeds the standards set forth in Health Current's Permitted Use Policy, the Participant (or its Business Associate) must submit a request in writing to its designated Health Current Account Manager. Health Current will treat the request as a request for a nonroutine disclosure under this procedure and respond accordingly.

Non-written requests or requests made to Health Current Workforce Members other than a Participant's designated Health Current Account Manager will impact and delay Health Current's ability to respond to the request. Participants understand and acknowledge that for a nonroutine request for access to be effective, Participants must submit the written request to their designated Health Current Account Manager.

4.2. Health Current's Uses, Disclosures or Requests of Data

4.2.1. Internal Uses

Health Current will limit its internal access and use of Data to its Health Current Workforce Members who require access to carry out their job responsibilities. Health Current Workforce Members will internally use the minimum amount of Data necessary for the particular Permitted Use.

4.2.2. Routine Disclosures or Requests

Most disclosures of or requests for Data that Health Current makes are part of providing routine services to Participants and their Business Associates. For example, disclosures or requests of Data for the following illustrative list of Permitted Uses are considered routine:

- 4.2.2.1. Treatment;
- 4.2.2.2. Payment;
- 4.2.2.3. Limited Health Care Operations;
- 4.2.2.4. Limited Public Health Activities;
- 4.2.2.5. Medical Examiner Activities;
- 4.2.2.6. Organ Procurement; and
- 4.2.2.7. The Health Current Permitted Use cases related to:
  - 4.2.2.7.1. Actions necessary to perform services under the Participation Agreement and to assist Participants (and their Business Associates) in the Permitted Uses;
  - 4.2.2.7.2. Taking action as directed in writing by a Data Supplier that has provided the Data; and

4.2.2.7.3. Conducting public health reporting, including (but not limited to) reporting of immunization data to the State of Arizona Immunization Registry.

4.3. Reasonable Reliance

In accordance with HIPAA, Health Current may reasonably rely on representations from the following categories of individuals and entities that only the minimum necessary amount of Data has been requested for routine and non-routine disclosures for Permitted Uses:

- **4.3.1.** A public official who represents that the Data requested is the minimum necessary for the official's purpose. If the public official makes this representation orally, Health Current will document this representation and retain such documentation in accordance with its record retention policy or procedure. Health Current Workforce Members will also verify the identity and authority of the public official.
- **4.3.2.** A Participant who is required to comply with HIPAA.
- **4.3.3.** A Business Associate who provides services to a Participant and who represents that the Data requested is the minimum amount necessary.
- **4.3.4.** A subcontractor of Health Current that assists Health Current in the performance of services for, or on behalf of, Participants or their Business Associates, and who represents that the Data requested is the minimum amount necessary.
- **4.3.5.** An individual or entity seeking Data for Research purposes that meets the federal and state requirements for Research.
- **4.3.6.** Participants, their Business Associates, and subcontractors of Health Current may make such representations orally, in writing or through their conduct, including (but not limited to) accessing the HIE, subscribing to alerts and so on.

Health Current will not rely on such a representation if it has independent knowledge that the request or disclosure would not meet the minimum necessary standard.

4.4. Nonroutine Disclosures or Requests

If Health Current receives a request for Data or it needs to request Data for a nonroutine purpose, Health Current will designate a Health Current Workforce Member to consult the Permitted Use Policy and underlying agreements to determine if the disclosure or request is permitted. If the nonroutine disclosure or request is permissible, the designated Workforce Member will make an individual determination of what amount of Data meets the minimum necessary standard in accordance with the requirements of the Permitted Use Policy, underlying agreements, HIPAA and this procedure.

For nonroutine **disclosures**, the designated Workforce Member will consider such factors as:

- **4.4.1.** The requestor's purpose in seeking Data;
- **4.4.2.** The specificity of the request (e.g., designating particular parts of an individual's medical record);
- **4.4.3.** Whether less Data, a Limited Data Set or De-identified Data would satisfy the purpose of the requestor; and
- **4.4.4.** Whether the requestor is an individual or entity upon which Health Current may rely, as set forth above.

For nonroutine **requests,** the designated Workforce Member will consider such factors as:

4.4.5. Health Current's purpose in seeking the Data and whether the request is sufficiently specific as to scope of the Data being sought (e.g., designating particular parts of a patient's medical record); and

4.4.6. Whether less Data, a Limited Data Set or De-identified Data would meet the purpose for the request.

The designated Workforce Member's determination will be documented and retained in accordance with Health Current's record retention policy or procedure.

4.5. Entire Medical Record

If permitted as set forth in Section 4.2.1 above, Health Current may reasonably rely on a requestor's representation that the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the Permitted Use. If a Health Current Workforce Member makes an independent determination that it is necessary to use, disclose or request an entire medical record for a Permitted Use subject to this Procedure, that Workforce Member will document the specific justification and retain a copy of the justification in accordance with Health Current's record retention policy and procedures.

5. Compliance

Health Current 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, Health Current may report such activities to applicable authorities.

6. Who Should Read this Policy?

6.1. Health Current HIE Participants

6.2. Health Current Staff

6.3. Health Current HIE Subcontractors

7. Reference/Citation

Embedded.

8. Cross Reference and/or Attachments

9. Revision Table

Version	Date	Description of Change	Revised By
A	1/26/2021	Initial Release	Board of Directors

NO INFORMATION BLOCKING POLICY

Document Name:	No Information Blocking Policy				
Document Code:	POL-ADM-0025-A			**Formerly:** (if applicable)	See below
Approval Authority:	Board of Directors	**Adopted:**	1/26/2021	**Reviewed: Frequency:**	Annually
Responsible Executive:	Melissa Kotrys	**Revised:**	See below		
Responsible Office:	Administration	**Contact:**	Melissa Kotrys		
Distribution:	**X** - Staff | **X-** Participants **X** – Vendors | **X** - Public	**Posted Locations:**	**X -** Internal Policy Library **X -** Public Website		

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

2. **Scope**
   This policy applies to Health Current and Participant Actors.

3. **Definitions**
   All capitalized terms in this HIE Participant Policy Manual will have the same meaning as provided in the Definitions Policy, in the Health Current Participation Agreement or HIPAA, all as amended from time to time.

   3.1 **Electronic Health Information (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.

   3.2 **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:

   3.2.1 The ability or means necessary to make EHI available for exchange or use (i.e., access to EHI),

3.2.2 The ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks (i.e., exchange of EHI); and/or

3.2.3 The ability for EHI, once accessed or exchanged, to be understood and acted upon (i.e., use of EHI).

3.3 **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).

3.4 **Safe Harbor** refers to a regulatory exception to the Information Blocking Rule, see 45 C.F.R. Part 171.

4. Policy

4.1. Compliance with the Information Blocking Rule

4.1.1. Health Current 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.

4.1.2. Health Current 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 Health Current or Participant Actors from engaging in practices that are Required by Law or that fall within a Safe Harbor. Health Current 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.

4.2. 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.

4.2.1. 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.

4.2.2. 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.

4.2.3. 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.

4.2.4. 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.

4.2.5. 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.

4.2.6. 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.

4.2.7. 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.

4.2.8. 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.

4.3. Information Blocking Complaints

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

4.3.2. Health Current 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.

4.3.3. Participant Actors must cooperate with Health Current in any investigation into a complaint of Information Blocking, including providing upon reasonable request by Health Current 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.

5. Compliance

Health Current 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, Health Current may report such activities to applicable authorities.

6. Who Should Read this Policy?

6.1. Health Current HIE Participants
6.2. Health Current Staff
6.3. Health Current HIE Subcontractors

7. Reference/Citation

Embedded.

8. Cross Reference and/or Attachments

9. Revision Table

Version	Date	Description of Change	Revised By
A	1/26/2021	Initial Release	Board of Directors

INDIVIDUAL RIGHTS POLICY

Document Name:	Individual Rights Policy				
Document Code:	POL-ADM-0026-A			**Formerly:** (if applicable)	See below
Approval Authority:	Board of Directors	**Adopted:**	1/26/2021	**Review: Frequency:**	Annually
Responsible Executive:	Melissa Kotrys	**Revised:**	See below		
Responsible Office:	Administration	**Contact:**	Melissa Kotrys		
Distribution:	**X** - Staff | **X**-Participants **X** – Vendors | **X** - Public	**Posted Locations:**	**X** - Internal Policy Library **X** - Public Website		

10. Purpose

Individuals have certain rights with respect to their health information, including a right of access, amendment, and an accounting of certain disclosures. The purpose of this policy is to describe how Health Current and Participants will work together to honor individual rights with respect to Data that is accessible through the HIE.

11. Scope

This policy applies to Health Current and Participants.

12. Definitions

See Definitions Policy.

13. Policy

13.1. Individual Access Requests

Individuals have a right to request a copy of their Data that is accessible through the HIE, see A.R.S. § 36-3802. Federal laws, like HIPAA, also gives individuals the right to access their health information, unless an exception to the individual's right of access applies. To request a copy of their Data, individuals (or an individual's personal representative) must complete a Health Information Request Form and return it to a Healthcare Provider Participant. Due to legal, technical, and administrative limitations, the HIE does not currently support alternative means by which individuals may access their Data through the HIE, such as through an individual access portal or other automated means.

13.1.1. Participant Responsibilities

13.1.1.1. **All Participants**

Because Health Current does not have a direct relationship with individuals whose Data is accessible through the HIE, Health Current must rely upon its Participants to verify that the individual who is requesting access either is the individual or personal representative of the individual. Thus, Participants must:

13.1.1.1.1. Accept an individual's completed Health Information Request Form;

13.1.1.1.2. Verify the identity and authority of the individual in accordance Applicable Law and healthcare industry standard security practices; and

13.1.1.1.3. Securely send the completed and validated Health Information Request Form to Health Current for processing.

13.1.1.2. **Data Suppliers (except for Part 2 Program Data Suppliers)**

This section does not apply to Part 2 Program Data Suppliers. Due to the sensitive nature of Part 2 Data and Part 2 compliance considerations, Part 2 Program Data Suppliers must follow the procedure set forth in the section of the policies titled Part 2 Program Data Supplier Responsibilities. If applicable, Data Suppliers that direct Health Current to deny an individual's access request partially or wholly may only do so if:

13.1.1.2.1. The denial is permitted by Applicable Law; and

13.1.1.2.2. The Data Supplier giving the direction provides the individual with the right to have the decision reviewed and considered for reversal (if Applicable Law affords the individual such rights).

In these circumstances, such Data Suppliers must provide a written explanation to Health Current for the denial within ten (10) calendar days of being notified of the access request. The written explanation must include at least the following information:

13.1.1.2.3. Data Subject to the Denial. A detailed and specific description of the Data to withhold, including the Data elements (such as diagnosis and progress notes). The Data Supplier is responsible for ensuring that the Data withheld is no more than reasonably necessary based on the reason for the denial.

13.1.1.2.4. Reason for the Denial. A statement explaining why the Data is being withheld. Examples include but are not limited to the following:

13.1.1.2.4.1. The person requesting access is not the individual or the individual's personal representative.

13.1.1.2.4.2. The person requesting access lacks the legal authority to access all the Data requested. For example, a minor child's parent/guardian may be entitled to access the minor's Data, except for Data related to healthcare services to which the minor child lawfully consented.

13.1.1.2.4.3. Permitting access would be reasonably likely to cause a substantial risk of harm to a natural person.

13.1.1.2.5. Preventing Harm. If the reason for the denial is preventing harm to a natural person, the written explanation must also include a statement that either:

13.1.1.2.5.1. Individualized Professional Determination. A licensed healthcare professional who has a current or past clinician-patient relationship has made an individualized determination, using professional judgment, that providing access to the individual (or personal representative who is requesting access) would substantially reduce a risk of harm to a natural person that would otherwise arise from giving access. The statement must also include one of the following regarding the risk of harm:

13.1.1.2.5.1.1. If the individual is the one requesting access, and the access denial relates to information about that individual, the professional's reasonable belief that providing access is reasonably likely to endanger the life or physical safety of the individual or another person;

13.1.1.2.5.1.2. If a personal representative is the one requesting access, the professional's reasonable belief that providing access is reasonably likely to cause substantial harm to the individual or another person; or

13.1.1.2.5.1.3. If the access denial relates to information about a person other than the individual who is the subject of the access request, the professional's reasonable belief that providing access is reasonably likely to cause substantial harm to that person.

The statement must include the name of the professional who made the determination and that professional's contact information; OR

13.1.1.2.5.2. Data Corruption. The Data which is requested is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason.

13.1.1.2.6. Review of the Decision. Information about how the requestor may seek to have the denial reviewed or, if applicable, an explanation of why the requestor does not have a right to have the denial reviewed under Applicable Law.

In the event the circumstances warrant a partial denial, and Health Current cannot segment the Data subject to the partial denial from the rest of the individual's Data, each affected Data Supplier is responsible for responding separately to the individual access request with respect to the Data each affected Data Supplier supplies to the HIE. Each affected Data Supplier must respond in the manner and within the time frame required by Applicable Law.

13.1.1.3. **Part 2 Program Data Supplier Responsibilities**
Health Current segregates Part 2 Data from other Data in the HIE because of its sensitive nature and Part 2's heightened privacy protections. For example, Part 2 imposes more stringent requirements on when an individual's personal representative may have access to an individual's Part 2 Data. Accordingly, Health Current will notify an individual's Part 2 Program Data Suppliers of an individual's access request, and each Part 2 Program Data Supplier is responsible for responding to the request in the manner and within the time frame required by Applicable Law.

13.1.2. Health Current Responsibilities
Health Current will respond to an individual access request within thirty (30) calendar days of receiving the completed and validated Health Information Request Form from the Participant. As permitted by Applicable Law and the Participation Agreement, Health Current may notify affected Data Suppliers of the individual access request, require the affected Data Suppliers to evaluate the request, and/or require the affected Data Suppliers to provide the requested access directly to the requestor.

Health Current may respond in writing to the individual access request by:

13.1.2.1. Providing the requestor with the requested Data;
13.1.2.2. Informing the individual that the individual's Data Suppliers will respond substantively to the request;
13.1.2.3. If permitted by Applicable Law, partially or wholly denying the request for access; or
13.1.2.4. Otherwise responding in a manner permitted by Applicable Law.

Health Current may partially or wholly deny an individual's request for access under the following circumstances, including but not limited to:

13.1.2.5. Health Current is not able to match the individual to Data in the HIE within accepted healthcare industry standards of accuracy, including if the Health Information Request Form submitted lacks the necessary demographic information about the individual or was not validated by the Participant.
13.1.2.6. If Health Current is instructed by the individual's Data Supplier(s) to deny the access request partially or wholly. Health Current will rely upon the Data Supplier's determination until such time as Health Current is notified by the Data Supplier that the determination has been reversed or revised.
13.1.2.7. Health Current reasonably believes that the denial will substantially reduce a risk of harm to a natural person that would otherwise arise from granting the access request, because the Data which is requested is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason. The scope of the denial will be no broader than necessary to substantially reduce the applicable risk of harm.

In the event the circumstances warrant a partial denial of an individual's access request, Health Current may deny the entire access request if it is not feasible for Health Current

to segment the Data subject to the partial denial from the rest of the Data. In such circumstances, each of the individual's Data Suppliers is responsible for responding to the request in the manner and within the time frame required by Applicable Law.

13.2. Individual Amendment Requests

Individuals have a right to request amendment to their Data that is accessible through the HIE, see A.R.S. § 36-3802. HIPAA also gives individuals the right to request amendment to their health information. Health Current has no authority or control over the accuracy or completeness of Data provided by Data Suppliers. Health Current will notify affected Data Suppliers if Health Current receives an amendment request directly from an individual (or an individual's personal representative). Data Suppliers are responsible for responding to individual amendment requests in the manner and within the timeframe required by Applicable Law.

13.3. Individual Accounting Requests

Individuals have a right to request a list of the persons who have accessed the individual's Data through the HIE for a period of at least three (3) years before the individual's request, see A.R.S. § 36-3802. HIPAA also gives individuals the right to request an accounting of certain types of health information disclosures. To request a list of the persons who have accessed their Data, Individuals must complete a Health Information Request Form and return it to a Healthcare Provider Participant.

13.3.1. Participant Responsibilities

Because Health Current does not have a direct relationship with individuals whose Data is accessible through the HIE, Health Current must rely upon its Participants to verify that the individual who is making the request either is the individual or personal representative of the individual. Thus, Participants must:

13.3.1.1. Accept an individual's completed Health Information Request Form;

13.3.1.2. Verify the identity and authority of the individual in accordance with Applicable Law and healthcare industry standard security practices; and

13.3.1.3. Securely send the completed and validated Health Information Request Form to Health Current for processing.

13.3.2. Health Current Responsibilities

Health Current will respond to an individual accounting request within thirty (30) days of receiving the completed and validated Health Information Request Form from the Participant.

14. Compliance

Health Current 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, Health Current may report such activities to applicable authorities.

15. Who Should Read this Policy?

6.1 Health Current HIE Participants
6.2 Health Current Staff
6.3 Health Current HIE Subcontractors

16. Reference/Citation
Embedded.

17. Cross Reference and/or Attachments

18. Revision Table

Version	Date	Description of Change	Revised By
A	1/26/2021	Initial Release	Board of Directors

HIE SECURITY AND MAINTENANCE POLICY

Document Name:	HIE Security and Maintenance Policy				
Document Code:	POL-ADM-0027-A			**Formerly:** (if applicable)	See below
Approval Authority:	Board of Directors	**Adopted:**	1/26/2021	**Reviewed: Frequency:**	Annually
Responsible Executive:	Melissa Kotrys	**Revised:**	See below		
Responsible Office:	Administration	**Contact:**	Melissa Kotrys		
Distribution:	**X** - Staff | **X**- Participants **X** – Vendors | **X** - Public	**Posted Locations:**	**X** - Internal Policy Library **X** - Public Website		

1. **Purpose**
   The purpose of this policy is to describe the security and maintenance practices that are reasonable and necessary to protect the confidentiality, integrity, and availability of Data, and to maintain and improve the health IT performance of the HIE.

2. **Scope**
   This policy applies to Health Current and Participants.

3. **Definitions**
   See Definitions Policy.

4. **Policy**
   - **4.1. Security Procedures**
     - **4.1.1.** Health Current and Participants are committed to Data security. In connection with HIE services, Health Current 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 Participation Agreement, and best security practices in the healthcare industry.
     - **4.1.2.** Participants must also follow Health Current'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 Data by mitigating the risk of access by unauthorized persons, see 45 C.F.R. 164 Subpart C.

4.2. HIE Downtime, Maintenance and Updates

4.2.1. For the HIE to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that the HIE 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 Health Current to take similar action with respect to the entire system or to specific Participants affected by a security or Data corruption/technical error.

4.2.2. Consistent with Health Current's obligations in the Participation Agreement, 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:

4.2.2.1. Performing routine (e.g., weekly) scheduled maintenance;
4.2.2.2. Performing scheduled updates;
4.2.2.3. 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;
4.2.2.4. Performing batch updates to patient or member panels or other Data ques necessary to HIE operations;
4.2.2.5. Addressing suspected or mitigating known security incidents;
4.2.2.6. As a result of serious environmental or other events; or
4.2.2.7. 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.

5. Compliance

Health Current 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, Health Current may report such activities to applicable authorities.

6. Who Should Read this Policy?

6.1 Health Current HIE Participants
6.2 Health Current Staff
6.3 Health Current HIE Subcontractors

7. Reference/Citation

Embedded.

8. Cross Reference and/or Attachments

9. Revision Table

Version	Date	Description of Change	Revised By
A	1/26/2021	Initial Release	Board of Directors