

## Response to Attachment A: Information Required to Complete Application

### SECTION III

#### Question 2-Catchment Area

All counties reflected in the map are indicative of intended, future service areas. All other communities are supported by entities with a current Nebraska Participation Agreement.

#### Question 3-Consumer Input

Customer service for consumers is addressed the same way it is for participants. Any questions or service requests, including opt outs, come in through our website, phone or email to the Support Desk. CyncHealth Support Desk personnel then triage the issue to the appropriate CyncHealth Team for a response and resolution.

#### Question 3-Closed-Loop Referral Service

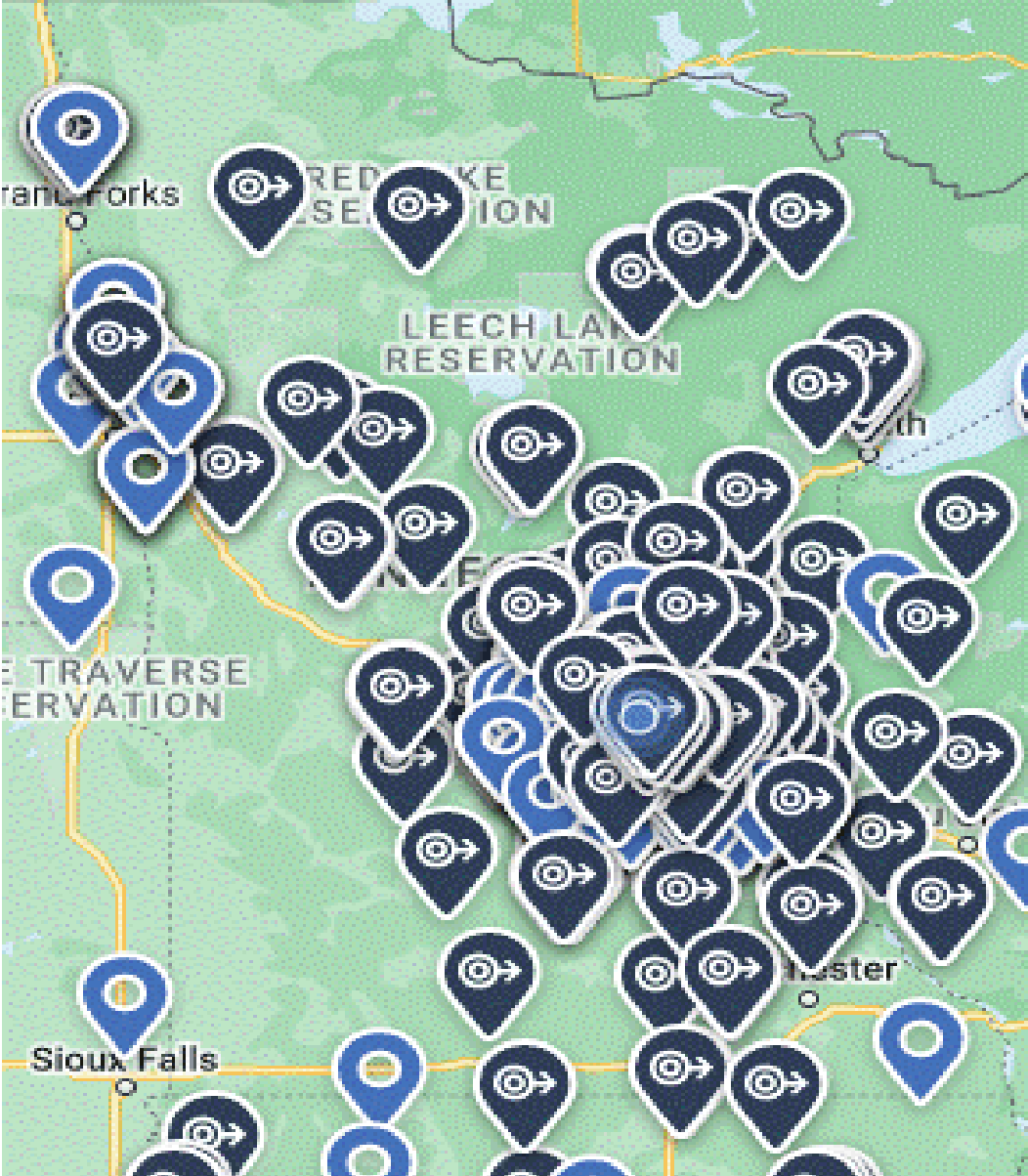
CyncHealth's social care platform is powered by Unite Us, and an independent platform from the Health Information Exchange (HIE) in Minnesota. CyncHealth's platform aligns healthcare and social care, engages community members, tracks outcomes, and sends and receives referrals based on individual needs. CyncHealth supported the social care platform in ten states in partnership with Unite Us using federal Support Act funding for implementation, this project was independent of being a state sponsored HIE for Nebraska and now Iowa and state certified HIE in Kansas.

Within the platform, users can:

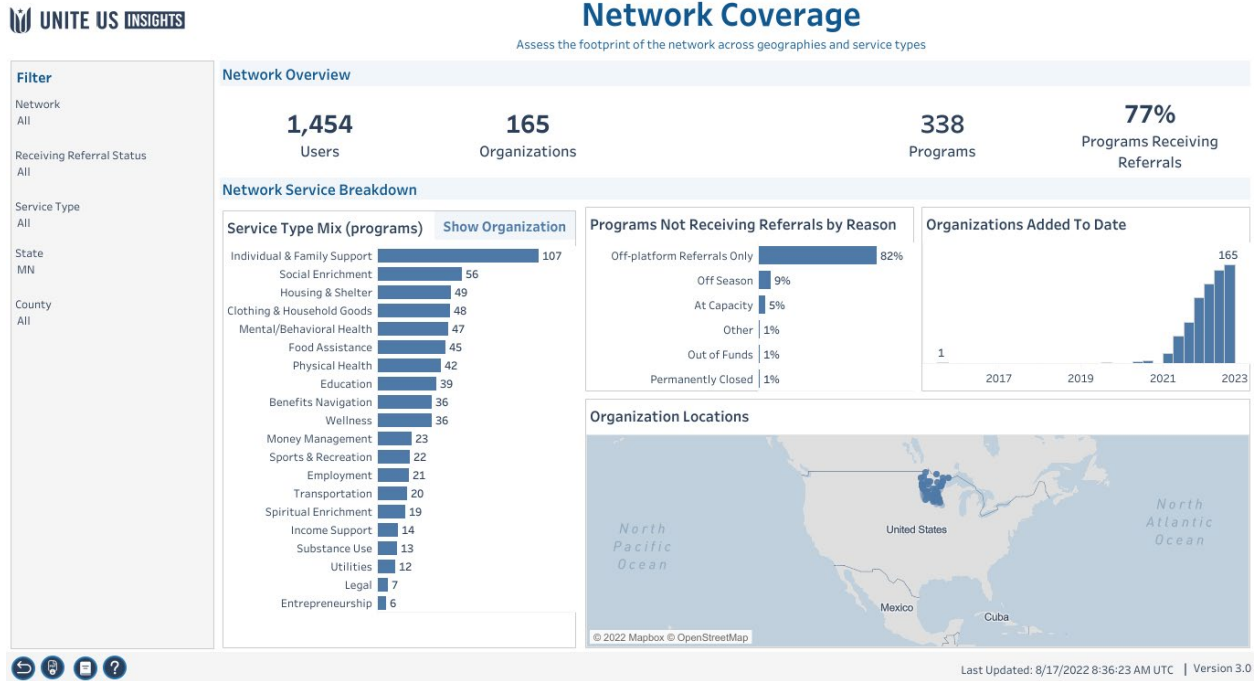
- Screen for social needs to address barriers to care and increase health equity.
- Connect individuals with resources including food, housing, transportation, mental health support, state benefits, and employment services.
- Refer and connect patients to currently available local services.
- Improve collaboration with a wide array of community partners.
- Track the outcomes of referrals and services delivered.
- Improve capacity through accurate referrals and data on local service delivery.

Figure 1 below is a 2022 map demonstrating the Unite Minnesota connectivity and Figure 2 highlights the services provided in the Minnesota area. Table 1 lists 2022 Community Based Organizations on the social care platform. Individuals residing on in border communities can receive services based on most convenient location, we have Community Based Organizations in border states.

Figure 1: Unite Minnesota Coverage



**Figure 2: Unite Minnesota Services**



**Table 1: Minnesota Community Based Organizations**

Name	City
Hope House of St. Croix Valley	Stillwater
Fraser	Woodbury
Warriors Next Adventure	St Paul
Military Appreciation Fund	Red Wing
Hunger Solutions	Red Wing
Helmets to Hard Hats	Red Wing

University of Minn.	Red Wing
Silent Warrior Project	Red Wing
Military Family Foundation	Red Wing
New Creations	Hugo
Faith City Church	St Paul
Homeownership Center	St Paul
East Side Neighborhood Development Company	St Paul
Guiding Star	St Paul
MN Network Hub	St Paul
Heartsprings Community Center	St Paul
Women for HER	St Paul
Giving Hope	St Paul
Christian Adoption Services	St Paul
Global Friends Coalition	St Paul
Family Development Center	St Paul
Breaking Free	St Paul
Minnesota Assistance Council for Veterans	St Paul
Caring Bridge	Eagle
Dress for Success	St Paul
PCs for People	St Paul

Epilepsy Foundation	St Paul
Harvest Pack	St Paul
Small Sums	St Paul
Beyond the Yellow Ribbon	Circle Pines, Plymouth
Freedom Fishing Foundation	Circle Pines
Loaves and Fishes	Minneapolis
CAPI	Minneapolis
Neighborhood Health Source	Minneapolis
Isuroon	Minneapolis
Open Arms	Minneapolis
GMCC	Minneapolis
Mile in My Shoes	Minneapolis
NeedyMeds	Minneapolis
Alexandra's House	Minneapolis
Veteran Sisters	Minneapolis
Angel Aid	Minneapolis
Military Family Network	Minneapolis
Culinary Hospitality Outreach and Wellness	Minneapolis
United through Reading	Minneapolis
Cute Syndrome Foundation	Minneapolis
Face It Together	Minneapolis

Help Now	Minneapolis
Lasagna Love	Minneapolis
Every Kid	Minneapolis
Giving Kitchen	Minneapolis
Hire Heros	Minneapolis
Upwardly Global	Minneapolis
Veterans Voices	Minneapolis
Child Neurology Foundation	Minneapolis
Give us the Floor	Minneapolis
Angel Flight	Minneapolis
Give Us	Minneapolis
Project Got Your Back	Minneapolis
Cancer Hope	Minneapolis
Urban Ventures	Minneapolis
Advocates for Thriving Communities	Minneapolis
Minnesota Community of African People with Disabilities	Minneapolis
Good in the Hood	Bloomington
Southside Community Health	Minneapolis
Cooper law	Minneapolis
Source MN	Minneapolis
Adult and Teen Challenge	Minneapolis

WellShare	Minneapolis
Community and Technical College	Minneapolis
Pregnancy Choices	Minneapolis
CARE Resource Connection	Fridley
Crossroads Panorama	Richfield
Raise the BARR	Minneapolis
Chefs for Seniors	Minneapolis
Twin Cities Rise	Minneapolis
Cars for Neighbors	Blaine
Community Partnership Collaborative	Minneapolis
Humanity Alliance	Minneapolis
Church of the Risen Savior	Burnsville
TEAM Wellness at Work	Minneapolis
EAGLE Group	Minneapolis
Sage Academy	Brooklyn Park
Hidden Resources for People of Color	Bloomington
Second Harvest Heartland	Minneapolis
Trinity Church	Lakeville
March of Dimes	Edina
UHC	Hopkins
Can Do Canines	New Hope

Star Legacy	Eden Prairie
Laura Baker Services	Northfield
START Senior Solutions	Eden Prairie
Serenity Health Advisors	Osseo
Southwest Transit	Eden Prairie
Academy of Whole Learning	Minnetonka
FISH Partner Network	Prior Lake
Youth First Community of Promise	Ramsey
Wings for Widows	Wayzata
Magnus Veterans Foundation	Dayton
The Community	Barronett
A Better Society	Chanhausen
His House	Excelsior
Chaska TreeHouse	Chaska
Intermission	Elk River
Hope Chest	Wayzata
Shepard of the Hill	Chaska
St John's Lutheran Church	Chaska
River Valley Health Services	Chaska
Prism Networking	Spring Park
Carver County	Chaska



Beyond New Beginnings	Chaska
Launch Ministry	Chaska
Grace Church	Chaska
Love INC	Chaska
Bountiful Basket	Chaska
Western Communities Action Network	Mound
Waconia United Food Shelf	Waconia
Life Care Unites	Waconia
Farm Rescue	Waconia
West unions Lutheran Church	Cologne
Healing Hearts	Big Lake
Southern Valley Alliance	Belle Plaine
Belle Plaine Food Shelf	Belle Plaine
Serenity Mental Health Services	Buffalo
Center for Suicide Awareness	Winter
Harmony Public Library	Harmony
Olivia Hospital	Hector
WebMed Mental health	Cloquet
23 <sup>rd</sup> Veteran	Duluth
Lincoln Park Collaborative	Duluth
College of St. Scholastica	Duluth

Fruit of the Vine	Duluth
Rural Psychiatry Associates	Renville
Safe families for Children	Alexandria
Car Care Program	Alexandria
Adult Basic Education	Alexandria
Outreach food Shelf	Alexandria
Knute Nelson	Alexandria
Prairie Five Community Action Council	Benson
Life Connections	Alexandria
Alomere Health	Alexandria
W. Central MN Communities Action	Alexandria
Prime West Health	Alexandria
Region 4 Mental Health Consortium	Alexandria
RuneStone Alternative	Alexandria
HFH of Douglas County	Alexandria
Horizon Public Health	Alexandria
PLUS Kids	Alexandria
Love INC	Alexandria
Minnewaska Lutheran Home	Starbuck
Minnewaska Community Health	Starbuck
Rainbow Rider	Lowry

#### **Question 4- Access and Query Ability**

Organizations who are covered entities are eligible to participate in the CyncHealth HIE for the state. Covered entities (e.g., hospitals, clinics) identify providers and delegates able to access the HIE for the organization. The participant receives log in credentials aligned to the specific covered entity organization who completed the participation agreement. Additionally, CyncHealth participates in eHealth Exchange allowing participating HIEs to connect as appropriate. The information from participant organizations that populates the HIE includes encounter information, diagnosis, diagnostic testing results, laboratory results, vital signs, immunization information, and care notes. The provider portal is the location where a participant accesses information about a patient. The aggregated data allows streamlined access to patient information.

CyncHealth is compliant with Minnesota Record Locator or Patient Information Service requirements (Minn. Stat. 144.291 sub.2 (i) and Minn. Stat. 144.293 sub.8) through our participant onboarding and privacy and security policies. Provider is defined under Minnesota law (144.291(i)) and CyncHealth will maintain an audit log of providers accessing the HIE, for which patient and the date of access for each access. The Minnesota Participant Agreement will require Authorized Users to comply with 144.291(2)(i) in the definition of Authorized User in accordance with 144.293(8).

CyncHealth will meet the “Conspicuous check box” requirement for opt-out of a record locator service by requiring patient consent by the participant organizations (see Attachment A “Minnesota Participant Agreement” and Attachment B “Minnesota Privacy Policies”). The documents describe the requirement of the participating organization to include the check box and the notice of disclosure to CyncHealth in the Provider’s Notice of Privacy Practices. Additionally, CyncHealth has a separate opt out process individuals can request (see Attachment C “Consumer Opt-Out Procedure” and Attachment D “Opt-Out Policy”)

The CyncHealth Privacy Program is a hallmark of our privacy and security practices. As previously mentioned, patient consent is required to be managed by the participant. However, CyncHealth has an additional opt out process for individuals.

#### **Question 5- Data Aggregation**

Only organizations who are covered entities are eligible to participate in the CyncHealth HIE for the state. Covered entities (e.g., hospitals, clinics) identify providers and their delegates able to access the HIE for the organization’s treatment purposes. The participant receives log in credentials aligned to the specific covered entity organization who completed the participation agreement. The provider portal is the only location where a participant accesses information about a patient. The aggregated data allows streamlined access to patient information.

Minnesota requirements are addressed in relevant governance policies, including terms within our Minnesota Participation Agreement and accompanying privacy policies (see Attachment A “Minnesota Participant Agreement” and Attachment B “Minnesota Privacy Policies”). These policies also describe limits on the use of information for treatment, payment, and operations (TPO), and the limiting nature of export or storage of information. Specifically, the CyncHealth platform prohibits printing or export of patient health information and only permitted uses are allowed for data within the provider portal.

## SECTION IV

### Appendix A-Item 1-Bylaws

Consistent with the CyncHealth practices for a state specific HIE, CyncHealth Minnesota would seek, invite, and include Minnesota representatives on the Board of Directors for the Minnesota HIE when it became operational and sustainable through state participation fees or other funding sources. Generally, relevant board members include stakeholders from hospitals and health systems and public health and/or Medicaid in relevant jurisdictions. CyncHealth has had success by partnering with local hospital and healthcare associations to identify key stakeholders important to success of a state HIE. For participation on the current CyncHealth Board of Directors, the bylaws could be amended to accommodate an additional representative from Minnesota. Likewise, guests can join the board for specified business-related topics on a case-by-case basis currently.

As shown in Appendix A, the composition of the CyncHealth Nebraska Board includes 24 members. At the time, there was a vacancy in the Class A membership, with recruiting efforts occurring throughout 2022. Additionally, some Class B members and the State of Nebraska had not appointed their representatives to the board. Recruitment efforts are always ongoing to ensure robustness and relevancy to the board and board members aware of the current vacancies and needs.

In addition to the Board of Directors, the CyncHealth enterprise has additional standing committees. All current committees are active and engaged in operations of the HIE, including the Executive and Finance Committee that includes Chief Financial Officers from different participating organizations who oversee the sustainability and stewardship of the organization. Likewise, the Compliance & Cybersecurity Committee is active and comprised of a number of consumers of the HIE representing a diverse discipline of compliance officers, security representatives, Chief Information Officers, as well as representing a diverse consumer stakeholder composition from payer, hospital, and academic facilities. The Data Governance Committee is guided by CyncHealth policies and procedures developed in partnership with leading industry consultants on privacy and security. This internal committee reviews data uses aligned with HIPAA, state legislation, and other applicable law for purposes of use to support

public health, quality improvement, and other needs. New data use cases are reviewed and debated by the committee which includes the Privacy Officer, Chief Information Security Officer, Chief Legal Counsel, Chief Data Officer, Chief Executive Officer and Chief Clinical Officer. Finally, due to low attendance and consumer burden, CyncHealth has ceased the Patient and Family Engagement Committee. The decision was determined appropriate given in Iowa and Nebraska patients cannot directly access the HIE, and “consumers” are providers identified by participating covered entities who often have their own Patient Advisory Committees. As needed, and relevant, CyncHealth would invite patient consumers as a guest or standing committee member.

### **Appendix A-Item 2-Certificate of Good Standing**

Please see Attachment E “Certificate of Good Standing.”

### **Appendix A-Item 3-Board Representation**

Currently, board members include stakeholders from hospitals and health systems and public health and/or Medicaid in relevant jurisdictions. As represented in the by-laws Class A and Class B members are recruited to provide representativeness across the continuum of care and the state to ensure effective and fair operations. While the CyncHealth Nebraska Board of Directors includes all Nebraska members except Michael White (who currently resides in Arizona but continues to be a representative from a Nebraska Hospital and academic medical center), the CyncHealth Iowa Board of Directors includes representative members across Iowa from varying organizational types. As stated above, CyncHealth practices for a state specific HIE include state representatives on the Board of Directors when participation and finding warrant a separate and state specific board. Generally, relevant board members include stakeholders from hospitals and health systems and public health and/or Medicaid in relevant jurisdictions.

### **Appendix A-Item 9-Strategic and Operational Plan**

Regardless of the state, CyncHealth leverages a formal governance structure and policies and processes that facilitate system goals. Governance creates the structure for an effective HIE and successful governance structures often have multiple layers to ensure balance and accountability. Our organization has three layers of governance, each with a unique focus but responsive to activities in the others. The HIE Board of Directors (BOD) oversees the strategic direction of the HIE and execution of operational activities. This board also approves other governance approaches and decisional processes. Second,

Our organization supports statewide interoperability through the exchange of data in near real-time at the point of care and in aggregate for population health management and policy support. In accordance with the standards set forth under HITRUST, as well as federal and state

statutory requirements, our organization is committed to ensuring the confidentiality, integrity, and availability of protected health information and electronic protected health information (PHI/ePHI), as well as any sensitive and confidential data it creates, receives, maintains, and/or transmits. With this in mind, all policies and procedures are designed to reduce risk to operations and enhance business prosperity. CyncHealth has vast internal policies for employee conduct and external policies for participants and procedures for data management, as shown in attachments.

Reliable technology is the foundation of CyncHealth. The technical architecture supports the foundational, exchange, and end-user services of the HIE. Our organization uses an interoperable platform to drive affordable and effective data exchange, across multiple vendors and data types. We use best-in-class health data platforms that allow data to flow through a componentized architecture capable of adapting to increasing volume, velocity, and veracity. enable complete results across the state. CyncHealth has extensive experience with integrating all major Electronic Health Records (EHR) vendors, utilizing all standards of communication and interoperability. We currently have over 100 connections with source systems, encompassing well over 500 individual location integrations, totaling over 2000 message type integrations. These integrations cover standard HL7 v2 interfaces, including but not limited to ADT, ORU ELR, RAD, VXU, and MDM, as well as other message types. Currently our integration engines process well over 2 million unique messages a day, expanding to well over 6 million messages sent outbound to downstream systems. Our reusable technical architecture adapts to increasing volume, velocity, and veracity. This purposed approach creates a foundation capable of supporting new work readily without unreasonable implementation costs and timelines.

CyncHealth subscribes to the IT Infrastructure Library (ITIL) framework to deliver consistent support to all participants for effective IT Service management (ITSM). ITIL enables us to handle issues and service requests efficiently by assigning clear roles and responsibilities to each of our support staff. Specifically, our support desk manages, organizes, automates, and responds to user questions and issues. Users can outreach to our support desk via online or telephone 24 hours per day, 7 days per week. Support desk personnel strive for first call resolution when possible and use an automated ticketing system for escalated needs. Service desk ticketing system is the single point of contact for end users to report any issue that affects their normal routine.

Additionally, the CyncHealth account management team excels at building relationships. Our teams work with facilities to explore needs and share our solutions. Once engaged, our team mentors participants through a proven model for facility onboarding. Facility onboarding is the coordination of facility connections to the health data utility systems and services. CyncHealth serves as the convener, supporting facilities to complete steps necessary for successful connections. The connections, in-turn, offer access to a core set of services needed for effective, efficient care coordination. Facility onboarding extends beyond the technical

connection, including account management services, post go-live technical assistance, education, and user engagement. The figure 3 demonstrates our facility onboarding cycle.

Specific to Minnesota, CyncHealth plans to engage facilities which previously expressed interest in HIE participation, such as border facilities and Nebraska health systems with a Minnesota presence. Approaching those with expressed interest ensures perceived value in participation for early network expansion. Concurrently, our account management team will begin outreaching to facilities in Minnesota already using our social care platform, Unite Minnesota. These facilities are familiar with CyncHealth approaches and find value in one of the health data utilities, suggesting an opportunity for deepening the connection with additional value through connected care and the longitudinal health record. Next, our account management team will begin promoting CyncHealth services and create brand awareness by presentations to local health systems, trade organizations, and community clinics. In most markets, our engagement path includes larger health systems, hospitals, clinics, government agencies, post-acute care facilities, and community-based organizations, respectively.

Overall, CyncHealth has years of experience in a reproducible onboarding process that can be leveraged in Minnesota. Our Account Management Team will initially engage potential participating organizations in Minnesota who already have connections in Iowa or Nebraska (e.g., Common Spirit, Unity Point). Next, our marketing and Participant Engagement team will deploy a market awareness campaign, to share information on advantages of participating in CyncHealth. As shown above, interested participants are easily onboarded to the network using reliable onboarding processes and scalable platforms already capable of supporting two statewide HIEs, and expanding on demand. Figure 4 shows a high-level onboarding roadmap.

CyncHealth is adept at scaling teams quickly to ensure successful onboarding in new markets. Key positions are monitored internally for potential resource allocation and external availability. CyncHealth has 69 fulltime positions with an additional 28 positions under various stages of recruitment. As a method to supplement our designated positions, we have arrangements with several staffing organizations to support our technical and administrative needs for short term or contract to hire positions (see Attachment F “Hiring Policy”). Most of our staff work at our main office in La Vista, Nebraska, however, we also have a satellite office in Des Moines, Iowa and Lincoln, Nebraska. Our model is to maintain a physical presence in locations where we operate a HIE with technical and account management staff to support local operations and enterprise staffing supporting satellite offices for legal, finance, and administrative needs.

Within the first operational year of the Minnesota HIE, CyncHealth will partner with potential stakeholders to identify a transparent and reasonable participant fee structure. Our fee structure is based on volume, using either a National Provider Identification (NPI) or Medicare hospital discharge count. This method ensures equitability in fees and participation regardless of annual budget (Critical Access Hospitals and community clinics pay a nominal fee currently). The fee structures are approved by the board annually (see Attachment G “Accounting Policy”). Since

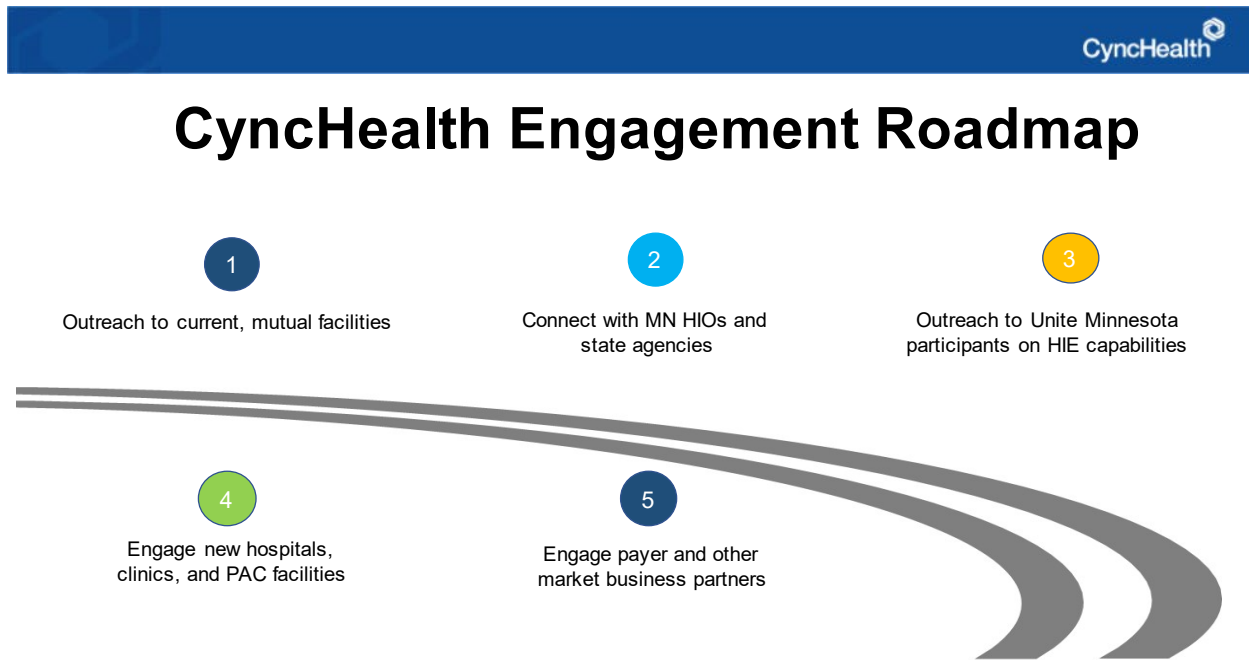
2009, our organization has maintained a sustainable funding model that includes balanced support from health plans, participants, and the State due to a significant value proposition. In addition to participation fees, CyncHealth is adept at securing federally funded opportunities and state and private scopes of work that offset participation fees. CyncHealth has received several million dollars in federal grants for health data and interoperability projects that benefit our overall technical architecture and enhance our service delivery model.

**Figure 3: Participant Engagement Cycle**





Figure 4: Minnesota Roadmap



As mentioned, CyncHealth uses Objectives and Key Results (OKRs) to guide our strategic activities throughout the year. Specific OKRs for Minnesota in the first quarters of the operational year are below.

1. Objective: Solidify business plan for Operating Year 1
  - a. Seek committee and board members across the Minnesota care continuum.
  - b. Refine funding and sustainability model to accommodate unique market characteristics.
  - c. Seek input from consumers and participants on value proposition and needs.
  - d. Connect with local trade organizations and advocacy groups.
  - e. Connect with state agencies on potential needs and use cases.
  - f. Convene participants and policy makers in planning health data utility infrastructure- this model is an emerging innovation that incorporates needs of people, providers, payers, policy makers and public health in governance, trust and utilization of data
  - g. Refine Minnesota participant outreach plan.
  - h. Engage currently interested participants with Account Management.

- i. Create onboarding roadmap.
  - j. Leverage modernized approaches to interoperability- API, FHIR, bulk FHIR
2. Objective: Solidify technical and operations plan for Operating Year 1
- a. Refine Minnesota technical infrastructure.
  - b. Develop relevant use cases, based on community feedback.
  - c. Offer demonstrations of HIE.

## SECTION V

### Appendix B-Question 2-Minnesota Participants

CyncHealth currently has no Minnesota participants to engage in quarter 1 or quarter 2 of 2023 per our OKRs and engagement roadmap above.

Due to the end of Support Act funding, CyncHealth will not onboard facilities separate from the HIE participation in 2023.

### Appendix B-Question 3-Minnesota Participants

As discussed above, CyncHealth engages participants in a variety of ways. One of the most significant manners is serving on the Board of Directors or other committees. Additionally, CyncHealth Account Management teams are continuously engaging participants in product demonstrations and discussion on value proposition and needs. All feedback is used to influence operations, products/services, and policies/procedures as relevant.

As mentioned above, CyncHealth has a robust customer service and participant experience program. Our Account Management Teams support participants throughout the lifecycle, including onboarding and trouble shooting needs. Our Service Desk is a robust approach to managing needs 24/7, using proven techniques. This supports our best-in-class service to customers which includes reliable, robust vendor partners and an extensible, interoperable platform.

## SECTION VI

### Organizational Response: Requirements

As discussed above, CyncHealth is compliant with Minnesota requirements (Minn. Stat. 144.291 sub.2 (i) and Minn. Stat. 144.293 sub.8) as outlined in our privacy policies. The Minnesota Participant Agreement will require Authorized Users to comply with 144.291(2)(i) in the definition of Authorized User in accordance with 144.293(8). CyncHealth will meet the “Conspicuous check box” requirement for opt-out of a record locator service by requiring patient consent from

the participant organizations (see Attachment A “Minnesota Participant Agreement” and Attachment B “Minnesota Privacy Policies”). The documents describe the requirement of the participating organization to include the check box and the notice of disclosure to CyncHealth in the Provider’s Notice of Privacy Practices. Additionally, CyncHealth has a separate opt out process individuals can request (see Attachment C “Consumer Opt-Out Procedure” and Attachment D “Opt-Out Policy”). The attachments describe Opt-Out processes and procedures for tracking information disclosures.

In addition to information provided by the participant organizations on Opt-Out, CyncHealth has a patient education brochure available both print and online (see Attachment G “Patient Education-English” and Attachment H “Patient Education-Spanish”). The brochures identify patient rights and processes for opt-out. Both brochures would be updated to reflect material unique to Minnesota and any updated logo.

If individuals, users, or participants request an audit, they may use the “User Audit Request Form” available through postal mail, electronic mail, or online (see Attachment I: “User Audit Request Form”). Once completed, CyncHealth uses the “Audit Standard Operating Procedure” to facilitate the request (see Attachment J “Audit Standard Operating Procedure”).

#### **Organizational Response: BAA**

CyncHealth has a dedicated policy analyst that tracks and identifies any rule changes that may affect CyncHealth. Our analyst works with the affected business groups to ensure that implementation of any rule changes are made by the required date. We have previously provided the BAA that CyncHealth signs with participants of the HIE and SDOH platform, which binds CyncHealth as a Business Associate to that Covered Entity. In addition, we have attached our subcontractor BAA which provides for the required contractual terms needed for anything CyncHealth may subcontract (see Attachment K “Subcontractor BAA”). Each of these contain all requirements of the 2013 Omnibus Rule.

**Attachment A  
Participation Agreement**



**Participant Name**  
**CYNCHHEALTH DATA SHARING**  
**PARTICIPATION AGREEMENT**  
**MINNESOTA**

TABLE OF CONTENTS

Definitions.....	3
Grant of Right to Use Services.....	4
Access to the System.....	5
Making Information Available through the System.....	9
Business Association Provisions.....	11
Participant’s Computer Systems.....	11
Policies and Procedures.....	11
Training.....	12
Fees and Charge.....	12
Confidential Information.....	13
Warranty, Disclaimer and Limitation of Liability, Indemnity.....	13
Insurance.....	16
Term; Modification; Suspension; Termination.....	16
Dispute Resolution.....	17
Applicable Law.....	17
Legal Compliance.....	17
No Assignment.....	17
Supervening Circumstances.....	17
Severability.....	18
Notice.....	18
Waiver.....	18
Complete Understanding.....	18
Signature Authority.....	18
No Medicare Exclusion.....	18
Rules of Construction.....	18
<b>Attachment 1: Services.....</b>	<b>20</b>
<b>Attachment 2: System.....</b>	<b>21</b>
<b>Attachment 3: DURSA Mandated Flow-Down Provisions.....</b>	<b>22</b>
<b>Attachment 4: Unite Us Platform Provisions.....</b>	<b>25</b>
<b>Attachment 5: InterSystems Mandated Flow-Down Provisions.....</b>	<b>27</b>
<b>Attachment 6: Fees.....</b>	<b>28</b>
<b>Attachment 7: Business Associate Agreement.....</b>	<b>29</b>
<b>Attachment 8: Additional Authorized Facilities.....</b>	<b>35</b>

**DATA SHARING  
PARTICIPATION AGREEMENT**

THIS DATA SHARING PARTICIPATION AGREEMENT is entered into by and between the Nebraska Health Information Initiative, Inc., DBA CyncHealth a Nebraska not-for-profit corporation (“CyncHealth”), and the undersigned participant (“Participant” or “County”) (collectively, the “Parties”), as of the date of last signature below (“Effective Date”).

**RECITALS**

CyncHealth is a not-for-profit corporation organized to improve the quality, safety, and timeliness of health services, reduce medical and prescription errors, and reduce health care costs by facilitating the exchange of health information in a manner that complies with all applicable laws and regulations, including, without limitation, those protecting the privacy and security of personal health information. CyncHealth has been **Certified by the State of Minnesota to operate a health information organization** for use by health care providers, health care payors, other covered entities, and other qualified entities to whom CyncHealth grants access in accordance with its policies and the law. The goal of the network is to support the public and charitable purposes of CyncHealth by improving public health and using technology to promote efficiency in the delivery of health care services.

Participant desires to have access to CyncHealth’s network and services.

In consideration of the mutual promises set forth in this Agreement, and other good and valuable consideration, the delivery and sufficiency of which is acknowledged, the Parties agree as follows:

**AGREEMENT**

**1. Definitions.** For the purposes of this Agreement, the terms set forth in this Article shall have the meanings assigned to them below. Terms not defined below (whether or not capitalized) shall have the definitions given them in HIPAA, unless the context requires otherwise.

“Affiliate” means any affiliates of CyncHealth, including CyncHealth Shared Services, Inc., the Nebraska Healthcare Collaborative, Inc., and any entity that is directly or indirectly controlled by, under common control with, or in control of CyncHealth.

“Agreement” means this Participation Agreement, as well as any Attachment selected above on the signature page, as all may be amended from time to time.

“Application” means Participant’s application to participate in the System, including all information furnished in any form in connection with the application.

“Authorized Users” means those members of Participant’s workforce (including employees, volunteers, members of its medical staff, and any other persons having access to the System by virtue of their relationship with Participant) who are individually authorized by Participant to have access rights to the System, **and in accordance with Minn. Stat. 144.291(2)(i) and Minn. Stat. 144.293(8)**, to assist Participant in providing treatment, obtaining payment for treatment, or conducting other permitted uses, and for whom a unique Participant ID has been assigned by Participant.

“Confidential Information” means, with respect to each party, any information concerning such party’s business, financial affairs, current or future products or technology, trade secrets, workforce, customers, or any other information that is treated or designated by such party as confidential or proprietary, or would reasonably be viewed as confidential or as having value to a competitor of such party. Confidential Information shall not include information that such party makes publicly available or that becomes known to the general public other than as a result of a breach of an obligation by the other party. Confidential Information does not include individuals’ health information.

“Electronic Health Information” means electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but shall not include (1) psychotherapy notes as defined in 45 CFR 164.501; or (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

“HIPAA” means the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d to 1320d-7, and future amendments thereto and the Regulations issued thereunder, including the Privacy Rule and the Security Rule.

“Participant ID” means a unique user identification assigned to an individual.

“Policies and Procedures” means CyncHealth’s rules, regulations, policies and procedures for access to and use of the System, including requirements related to the granting of Participant IDs and appropriate levels of System access to Authorized Users by the respective Participants and Direct Trust Certificate compliance, as from time to time posted electronically on the System or otherwise furnished to Participant in writing.



“Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

“Regulations” means the final Regulations implementing the privacy and security provisions of HIPAA as amended from time to time. The Regulations are presently codified at 45 C.F.R. Parts 160, 162, and 164.

“Security Incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

“Security Rule” means the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR part 160 and part 164, subparts A and C.

“Services” means the services listed in any Attachment to this Agreement.

“System” means the network and all software and hardware provided by CyncHealth.

“Term” means the initial term and all renewal terms of this Agreement.

## **2. Grant of Right to Use Services.**

2.1 Access. During the Term, CyncHealth grants to Participant and Participant accepts a non-exclusive, non-transferable (except as provided herein) right to have access to and to use the System and any related software. Such access and use is subject to Participant’s compliance with the terms and conditions set forth in this Agreement and with CyncHealth’s Policies and Procedures (“Policies and Procedures”), as provided in Article 7 below.

2.2 Restrictions. Participant shall obtain no rights to the System except for the limited rights to use the System expressly granted by this Agreement. Participant shall not:

- (a) Make the System or Services, in whole or in part, available to any other person, entity or business, other than as set forth in this Agreement;
- (b) Copy, reverse-engineer, decompile, or disassemble the System, in whole or in part, or otherwise attempt to discover the source code to the software used in the System; or,
- (c) Modify the System or combine the System with any other software or services not provided or approved by CyncHealth.

2.3 Change and Termination. CyncHealth reserves the right to change the System, Services, or standards for connectivity and/or end-user equipment, or to cease operating the System or any or all Services, at any time. Changes to the System or the Services that reduce or limit the functionality or levels of service provided shall not be made less than sixty (60) days prior notice to Participant, unless circumstances beyond CyncHealth's control require it.

2.4 Third-Party Software. The System includes certain Third-Party Software and Services which may require that Participant enter into separate subscription or licensing agreements with third-party vendors, or which may be open-source, as a condition of Participant's use of the System. If Participant elects not to execute agreements with such third-party vendors or determines it is unable to comply with the terms of any license or other agreement held by CyncHealth, Participant may elect to terminate this Agreement. This Agreement shall not be construed to limit any use of open-source Software in accordance with applicable software licenses

### 3. Access to the System.

3.1 Permitted Uses. Subject to the terms of this Agreement, CyncHealth authorizes Participant and its Authorized Users to access the System and to use the Services only as authorized in this Agreement. **These uses must be reflected in Participants notice to patients and the required consent under the Minnesota Health Records Act.**

#### (a) Limited Data Sets and Additional Uses.

(i) CyncHealth may create limited data sets from Participant's Shared Information and disclose them for any purpose for which Participant may disclose a limited data set without authorization, and Participant hereby authorizes CyncHealth to enter into data use agreements for the use of limited data sets, in accordance with Applicable Laws.

(ii) CyncHealth may use Participant's Shared Information to provide data aggregation services relating to Participant's and other users' health care operations in accordance with the Policies and Procedures

(iii) CyncHealth may create limited data sets from Participant's Shared Information, and disclose them for any purpose for which Participant may disclose a limited data set without authorization, and Participant hereby authorizes CyncHealth to enter into data use agreements for the use of limited data sets, in accordance with Applicable Laws and with the Policies and Procedures. Upon request, CyncHealth shall provide Participant with

reports listing recipients of limited data sets utilizing Participant's Shared Information, except that such reports shall not include disclosures of limited data sets to and through the Nebraska Healthcare Collaborative, Inc. (the "Collaborative").

(iv) CyncHealth may de-identify Participant's Shared Information and may make the de-identified information available to others, including the Collaborative, in accordance with the Policies and Procedures.

(v) CyncHealth and its Affiliates, including the Collaborative, may use Participant's Shared Information to provide data aggregation services relating to Participant's and other users' health care operations in accordance with the Policies and Procedures.

**3.2 Prohibited Uses.** Participant agrees not to access the System or use the Services for any other purpose other than as set forth in Section 3.1 above. In particular:

(a) Participant shall not reproduce, publish, or distribute content in connection with the System that infringes any third party's trademark, copyright, patent, trade secret, publicity, privacy, or other personal or proprietary right.

(b) Participant shall comply with all applicable laws, including laws relating to maintenance of privacy, security, and confidentiality of patient and other health information and the prohibition on the use of telecommunications facilities to transmit illegal, obscene, threatening, libelous, harassing or offensive messages, or otherwise unlawful material.

(c) Participant shall not:

(i) Abuse or misuse the System or Services, including gaining or attempting to gain unauthorized access to the System or altering or destroying information in the System, except in accordance with accepted practices;

(ii) Use the System or Services in such a manner that interferes with other users' use of the System; or,

(iii) Permit the introduction into the System of any program, routine, or data (such as viruses or worms) that does or may disrupt or impede the operation of the System or alter or destroy any data within it.

(d) Participant shall not knowingly:

(i) Abuse or misuse the System or the Services, including gaining or attempting to gain unauthorized access to the System or altering or destroying information in the System, except in accordance with the Policies and Procedures;

(ii) Grant access to a user, or provide a user with a level of access to the System, that is not permitted in compliance with HIPAA, Applicable Law, and the Policies and Procedures regarding access to protected health information;

(iii) Use the System or Services in such a manner that interferes with other users' use of the System; or, Introduce into the System any program, routine, or data (such as viruses or worms) that does or may disrupt or impede the operation of the System or alter or destroy any data within it.

### 3.3 Participant's Own Systems.

(a) Participant shall be responsible for its compliance with any applicable regulatory requirements related to the preservation, privacy, and security of its own records, including without limitation data backup, disaster recovery, and emergency mode operation, and acknowledges that CyncHealth does not provide such services.

(b) Participant may access and use the Electronic Health Information as permitted in this Agreement and may merge relevant parts of such Electronic Health Information into its own, in which case such merged data becomes the property of Participant to the extent thus incorporated into its record.

3.4 Data Aggregation and Subpoenas. If Participant is subpoenaed or otherwise ordered to use the System for the purpose of compiling the data of Other Participants that are not already contained in Participant's records, Participant shall immediately notify CyncHealth so that CyncHealth and such other interested parties as it may determine might have an opportunity to appear or intervene and protect their respective interest. Participant shall not be required to contest any such subpoena or order, nor incur any expense in connection with legal proceedings or processes, whether initiated by CyncHealth or any other interested party, with respect thereto.

### 3.5 Safeguards.

(a) Participant and CyncHealth shall implement and maintain appropriate

administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of Electronic Health Information accessible through the System, to protect it against reasonably anticipated threats or hazards, and to prevent its use or disclosure otherwise than as permitted by this Agreement or required by law.

(b) Participant shall promptly notify CyncHealth of any Security Incident relating to the System of which Participant becomes aware, any unauthorized use or disclosure of information within or obtained from the System, any inappropriate grant of access or assignment of access rights to Participant's Authorized Users, or any abuse of access or access rights by any of Participant's Authorized Users, and shall cooperate with CyncHealth in investigating the incident and shall take such action to mitigate any breach or suspected breach.

(c) Participant shall maintain appropriate security regarding all personnel, systems, and administrative processes used by Participant to transmit, store, and process Electronic Health Information through the use of the System. Participant shall establish appropriate security management procedures, security incident procedures, contingency plans, audit procedures, facility access controls, workstation use controls and security, device and media controls, authentication procedures, and security policies and procedures to protect Electronic Health Information accessible through the System.

(d) Each party shall immediately notify the other of any Security Incident relating to the System of which either party becomes aware, or any unauthorized use or disclosure of information within or obtained from the System and shall cooperate with each other in investigating the incident and shall take such action to mitigate any breach or suspected breach.

3.6 Compliance. Participant and CyncHealth, respectively, are responsible for their own compliance with the terms of this Agreement, HIPAA, the Policies and Procedures, and any Applicable Law including the Minnesota Health Records Act. Participant shall be solely responsible for the use of the System by Participant and Participant's workforce, or any business associate or contractor of Participant, who accesses and uses the System or Services as Authorized Users on its behalf, as well as the efficacy and appropriateness of granting access and access rights to Participant's workforce, business associates or contractors.

### 3.7 Authorized Use.

(a) Participant, or Participant's duly authorized agent, may assign Participant IDs and appropriate levels of access to the System to parties Participant designates as

Authorized Users. Such Participant IDs and access rights shall be granted by Participant pursuant to a role-based access and identity management process established by Participant, that is consistent with all requirements of HIPAA, Applicable Law, and the Policies and Procedures. The process for granting access shall be substantially similar to the process Participant utilizes for its own electronic medical record system. Participant shall ensure that each Authorized User has and uses his, her, or their own Participant ID and Participant shall adopt and maintain reasonable security precautions for Participant IDs to prevent disclosure to and use by unauthorized persons.

The authority to assign Participant IDs and grant use rights in the System does not convey any ownership rights in the System or Services to the Participant. CyncHealth may revoke or restrict assigned Participant IDs or use rights granted by Participant at CyncHealth's sole discretion.

(b) Participant's Authorized Users may only use the System and the Services on behalf of Participant subject to the terms of this Agreement. Participant shall:

(i) Provide a Participant ID for each Authorized User and take efforts to ensure that each such person has access to the System only under his or her assigned Participant ID;

(ii) Train all Authorized Users regarding the security and confidentiality requirements of this Agreement and the Policies and Procedures relating to their access to and use of the System and the Services, and be responsible for their compliance with such requirements;

(iii) Promptly notify CyncHealth of violations of the confidentiality requirements set forth in this Agreement by Participant's Authorized Users;

(iv) Promptly terminate any Participant ID and associated rights of access assigned to an Authorized User whose employment is terminated (or if the individual is not an employee, upon the termination of the relationship with Participant which permitted the individual to be granted access to the System) in the same manner in which Participant terminates users of its own electronic medical record and information systems under such circumstances.

(v) Take prompt steps to assure that any Authorized User whose access or access rights in the System have been revoked or restricted by Participant has no further access to protected health information through the System; and,

(vi) In the event CyncHealth notifies Participant of a Security Incident or other compliance concern involving an Authorized User, participate fully in any investigation of such Authorized User's access and use as necessary to determine the nature and extent of the Security Incident or compliance concern, and take any mitigating action necessary or otherwise required by CyncHealth to mitigate the effects of such Security Incident or compliance concern, up to and including revoking or restricting the access or access rights of the Authorized User.

3.8 Cooperation. Participant shall reasonably cooperate with CyncHealth in the administration of the System, including providing reasonable assistance in evaluating the System and collecting and reporting data requested by CyncHealth for purposes of administering the System.

3.9 Discipline and Terminate of Authorized Users.

(a) Participant shall require that all of its respective Authorized Users, including workforce, business associates, and contractors, who use or have access to the System and the Services do so only in accordance with applicable use restrictions and confidentiality obligations and the Policies and Procedures, including without limitation, the provisions thereof governing the confidentiality, privacy, and security of protected health information.

(b) Participant shall take appropriate disciplinary action, up to and including termination, against any of Participant's Authorized Users who violate their use restrictions, confidentiality obligations, or the Policies and Procedures. CyncHealth may require Participant to revoke or restrict the access and/or access rights of an Authorized User in the event CyncHealth or another Participant identifies inappropriate use or access by such Authorized User to the System or protected health information within the System which is in violation of HIPAA, Applicable Laws, or the Policies and Procedures, and if Participant fails to do so promptly, then Participant shall be considered to be in breach of this Agreement pursuant to Section 3.10 below.

3.10 Termination of a Participant. Following discussion with a Participant and a reasonable opportunity to cure (if such cure is possible), CyncHealth may terminate that Participant's access to the System on a temporary or permanent basis for privacy and security breaches or for failure to take reasonable remedial action when a breach is discovered, including, without limitation:

(a) Failure to cooperate in mitigating damages,

- (b) Failure to appropriately discipline an Authorized User or other person under the Participant's control for security or privacy violations,
- (c) Failure to promptly revoke or restrict access rights to the System of an Authorized User when requested by CyncHealth pursuant to Section 3.9 above; or,
- (d) Take other actions or fail to take actions that have the effect of undermining the confidence of Other Participants in the effectiveness of System safeguards.
- (e) CyncHealth shall explain to Participant the basis and support for terminating Participant's access.

3.11 Professional Responsibility. Participant shall be solely responsible for the medical, professional, and technical services it provides. CyncHealth makes no representations concerning the completeness, accuracy, or utility of any information in the System, or concerning the qualifications or competence of individuals who placed it there. CyncHealth has no liability for the consequences to Participant or Participant's patients of Participant's use of the System or the Services.

#### **4. Making Information Available through the System.**

4.1 Purpose of System. The purpose of the System is to facilitate the sharing of patient health information among all Participants.

4.2 Accuracy and Format of Data. Participant shall use reasonable efforts to ensure that Participant's Shared Information is current, accurate, and (subject to any restrictions imposed by law or this Agreement, including Section 4.8) complete, or if it is incomplete, that the record contains an appropriate indication to that effect and complies with any requirements of CyncHealth's data standards as to format or content.

4.3 Sharing of Participant's Shared Information. Participant authorizes CyncHealth to use and disclose Participant's Shared Information as follows, subject to the recipient's agreement to comply with the Policies and Procedures and with Applicable Laws and regulations relating to the use and disclosure of health information, and subject also to the provisions of this Agreement:

- (a) CyncHealth may permit access to Participant's Shared Information by Other Participants for treatment, payment and healthcare operations. Participant agrees that any disclosure pursuant to this section is a disclosure made by a Participant and not CyncHealth; and,



(b) CyncHealth may use and disclose Participant's Shared Information for the proper management and administration of CyncHealth and the System, and to carry out CyncHealth's legal responsibilities. CyncHealth may also disclose Participant's Shared Information for such purposes if the disclosure is required by law. Without limiting the foregoing, CyncHealth may permit access to the System by CyncHealth's authorized personnel. CyncHealth agrees that any disclosure pursuant to this section is a disclosure made by CyncHealth and not the Participant.

4.4 Reliance on Representations. Participant acknowledges that CyncHealth is relying on the assurances of Participant and the Other Participants that are granting access and access rights to the System to their respective Authorized Users, including but not limited to:

(a) That appropriate access and levels of access rights are being granted to their respective Authorized Users;

(b) That the purposes for which such Authorized Users are accessing the System are in compliance with HIPAA, Applicable Laws, and the Policies and Procedures; and,

(c) That the granting of access is being conducted pursuant to an appropriate identity and access management system utilized by each Participant.

Participant acknowledges that, while the System will contain certain technical safeguards against misuse of the System, it will rely on the representations and undertakings of its Authorized Users and the Other Participants and their Authorized Users. Participant agrees that CyncHealth shall not be responsible for any unlawful access to or use of Participant's Shared Information by Participant's Authorized Users or by any Other Participant or its Authorized Users.

4.5 Compliance with Privacy Rule. CyncHealth represents and warrants that the Policies and Procedures of CyncHealth relating to the generating of Participant IDs and the granting of appropriate access levels to Authorized Users of Participant are based on the standards of the Privacy Rule. Participant acknowledges that other federal and state laws impose additional restrictions on the use and disclosure of certain types of health information, or health information pertaining to certain classes of individuals. Participant is solely responsible for ensuring that Participant's Shared Information may properly be disclosed for the purposes set forth in this Agreement, whether under HIPAA or under such other federal and/or state laws.

In particular, Participant shall:

- (a) Not make available through the System any information subject to any restriction on use or disclosure (whether arising from Participant's agreement with the individual or under law), other than the general restrictions contained in the Privacy Rule;
- (b) Obtain any necessary consents, authorizations, or releases from individuals required for making their health information available through the System; and,
- (c) Include such statements (if any) in Participant's notice of privacy practices as may be required in connection with Participant's use of the System.

4.6 Individual Rights. Participant shall be solely responsible for affording individuals their rights with respect to Participant's Shared Information, such as the rights of access and amendment, or requests for special restrictions on the use or disclosure of health information. CyncHealth shall not accept or process any requests from individuals for the exercise of such rights, but shall promptly forward any such requests to Participant. Participant shall not undertake to afford an individual any rights with respect to any information in the System other than Participant's Shared Information.

4.7 Rights in Data. As between CyncHealth and Participant, all Authorized User Data shall be deemed to be the exclusive property of Participant. In no event shall CyncHealth claim any rights with respect to the Authorized User Data, use or authorize any third-party to use such data, or take any action with respect to such data that is inconsistent with this Agreement. CyncHealth hereby waives any and all statutory or common law liens it may now or hereafter have with respect to such Authorized User Data. Participant may retrieve, transport, and deliver to third parties the Authorized User Data, and all manipulations of such data associated with the System and Services and the Authorized User Data contained in CyncHealth's archived data files.

4.8 No Third-Party Access. Except as required by law, Participant shall not permit any third party (other than Participant's Authorized Users) to have access to the System or to use the Services without the prior written agreement of CyncHealth. Participant shall promptly notify CyncHealth of any order or demand for compulsory disclosure of health information that requires access to or use of the System. Participant shall cooperate fully with CyncHealth in connection with any such demand.

## **5. Business Associate Provisions.**

5.1 Compliance with Privacy and Security Rules. CyncHealth and Participant shall comply with the Privacy Rule and the Security Rule.

5.2 Business Associate Agreement. CyncHealth and Participant agree to the terms and conditions of the HIPAA Business Associate Agreement.

**6. Participant's Computer Systems.** In order to use the System, Participant acknowledges that it may be necessary for it to acquire, install, configure, and maintain equipment necessary to access the System listed or described in this agreement. Participant shall comply with the technical requirements. If CyncHealth notifies Participant that its equipment for the implementation and use of the System is incompatible with the System and not in accordance with the technical requirements, Participant shall either eliminate the incompatibility or terminate this Agreement and CyncHealth may suspend Services to Participant until Participant does so. Participant acknowledges that changes in Participant's computer systems or software, including changes in electronic health record (EHR) systems or software vendors, may require the establishment of a new connection to the System. Participant acknowledges that such changes may incur additional costs by Participant. In the event there is no state or federal funding opportunities available to assist in the cost of such changes to Participant's computer systems, software, or new connections, Participant shall be solely responsible to pay any additional costs directly to the EHR vendor.

**7. Policies and Procedures.** CyncHealth is solely responsible for the development of the Policies and Procedures and may amend, or repeal and replace, them at any time as CyncHealth determines is appropriate. CyncHealth generally shall notify Participant of any changes at least ninety (90) days prior to the implementation of the change. However, if the change is required in order for CyncHealth or Participant to comply with applicable laws or regulations, CyncHealth may implement the change and provide notice to Participant within a shorter period as determined appropriate by CyncHealth.

7.1 CyncHealth's Policies and Procedures, as they exist now or in the future, are incorporated herein by this reference and are made a part of this Agreement. This Agreement and the Policies and Procedures shall be construed wherever reasonable as being consistent with each other. In the event there is a material conflict between a provision of this Agreement and the Policies and Procedures, the terms of this Agreement shall control.

**8. Training.** Participant shall cause its personnel to participate, at Participant's cost and expense, in any training required by CyncHealth and any training necessary to be compliant under HIPAA or any applicable law for the storage, use or transmission of Protected Health Information.

## 9. Fees and Charges.

9.1 Service Fees. Participant shall pay CyncHealth the Service Fee set forth in Attachment 7 during the Term and any continuation of this Agreement. CyncHealth may change its Service Fee and Miscellaneous Charges upon thirty (30) days' written notice to Participant.

9.2 Payment. The Service Fee and any Miscellaneous Charges shall be due and payable to CyncHealth within thirty (30) days of receipt of invoice.

9.3 Taxes. All charges and fees shall be exclusive of all federal, state, municipal, or other government excise, sales, use, occupational, or like taxes now in force or enacted in the future. Participant agrees to pay any tax (excluding taxes on net income) that Participant may be required to collect or pay now or at any time in the future and that are imposed upon the sale or delivery of items and services purchased under this Agreement.

9.4 Funding Opportunity. If available, Participant may be able to leverage funding opportunities from the State of Nebraska and the Centers for Medicare and Medicaid ("CMS") to cover set up and implementation costs of connecting to CyncHealth. This funding is inclusive of vendor implementation costs and OID costs if paid by the Participant or covered by a coupon to register provided to Participant by CyncHealth. It does not include any Participant staff costs.

Such funding opportunity is timebound based on dates established via federal deadlines. Participant must be able to complete the project by the applicable funding deadline to leverage the funding opportunity. The project will be considered complete when the Participant's interface with the HIE is live and meets the latest published version of the USCDI. If Participant is not able to complete the project by the federal deadline Participant must provide written notice to CyncHealth at least thirty (30) days before the deadline.

Should the project be terminated because Participant or its vendor halts or unreasonably delays the Project, or otherwise did not fulfill its commitments as outlined in the project requirements Participant agrees to return any funding assistance, including implementation costs and OID costs provided or reimbursed by CyncHealth. Because these costs are covered by federal dollars, allocated for a specific purpose, if such designated purpose is abandoned, funds must be reallocated pursuant to federal HITECH funding mechanisms and requirements.

(a) Payment Information. To utilize such a funding opportunity, Participant shall provide CyncHealth an invoice for electronic health record ("EHR") vendor fees that match the agreed upon quote and appropriate OID costs for reimbursement.

(b) CyncHealth, through grant funding, pays the set and implementation costs. CyncHealth submits invoices to Nebraska's Department of Health and Human Services ("DHHS") for reimbursement on the 15th of each month. To have such invoices submitted by the 15th, Participant must provide said invoice by the 10th of the month. Upon DHHS approval of reimbursement, CyncHealth will be able to receive funds to provide Participant reimbursement for submitted invoice.

(c) Participant will pay for participation and all other services set forth in Attachment 7 as provided in this Section 9.

9.5 Funding Availability. CyncHealth or state and federal funders may terminate this project and/or the connection funding without penalty, in whole or in part, in the event funding is not received by CyncHealth or is no longer available from the associated funding source. CyncHealth shall give Participant thirty (30) days' written notice prior to the effective date of any such termination and CyncHealth shall have no further obligation regarding such funding.

9.6 No Payment for Protected Health Information. All fees charged, paid or collected by or on behalf of CyncHealth related to the System and the data contained therein shall be for the rights of Participants to access and use the System and Services as described in this Agreement. CyncHealth, including its Subcontractors, shall not make Participant's Shared Information or any individual's protected health information provided to CyncHealth by Participant available to any third party for any purpose not expressly authorized in this Agreement. Neither CyncHealth nor its Subcontractors shall offer to pay or solicit or receive any remuneration, directly or indirectly, in return for protected health information obtained through the System.

**10. Confidential Information.** Each Party shall not disclose the other Party's Confidential Information to any other person and shall not use any Confidential Information except for the purpose of this Agreement. Except as otherwise provided in this Agreement or other prior written consent, neither Party shall, at any time, directly or indirectly, divulge or disclose Confidential Information for its own benefit or for the purposes or benefit of any other person. Each Party agrees to hold all Confidential Information of the other party in strict confidence and shall take all measures necessary to prevent unauthorized copying, use, or disclosure of such information, and to keep the Confidential Information from falling into the public domain or into the possession of persons not bound to maintain the confidentiality of Confidential Information. Parties will disclose Confidential Information to those who need to know for the purpose of this Agreement. Parties shall inform all such recipients of the confidential nature of Confidential Information and will enter into a written agreement with them containing confidentiality restrictions no less restrictive than those set forth in this Agreement. Each Party shall promptly advise the other party in writing of any improper disclosure, misappropriation, or misuse of the other party's Confidential Information by any person, which may come to the Party's attention.

10.1 Equitable Relief. Each Party agrees that the other Party will suffer irreparable harm if the Party fails to comply with its obligations set forth in this Article 10, and further agrees that monetary damages will be inadequate to compensate the other Party for any such breach. Accordingly, each Party agrees that the other Party will, in addition to any other remedies available to it at law or in equity, be entitled to the issuance of injunctive relief to enforce the provisions hereof, immediately and without the necessity of posting a bond.

10.2 Survival. This Section 10 will survive the termination or expiration of this Agreement for any reason.

## **11. Warranty, Disclaimer and Limitation of Liability, Indemnity.**

11.1 Warranty. CyncHealth represents and warrants that the Services shall be provided according to this Agreement.

11.2 Pass-Through Warranty. To the extent assignable by CyncHealth to Participant, CyncHealth assigns and passes through to Participant, and Participant shall have the benefit of, any and all third-party warranties and indemnities pertaining to the System. If such warranties and indemnities made to CyncHealth are not assignable to Participant, and if the vendor provides no applicable warranties or indemnities directly to Participant, then during the term of this Agreement, CyncHealth shall use reasonable efforts to enforce for the benefit of Participant such applicable warranties and indemnities as are made by the vendor to CyncHealth. Participant understands and agrees that its sole remedy for the breach of any such warranty or indemnity shall be against the third-party vendor and not against CyncHealth, nor shall any such breach have any effect whatsoever on the rights and obligations of either Party with respect to this Agreement.

11.3 No Other Warranties. OTHER THAN AS SET FORTH IN THIS SECTION OR THE AGREEMENT, THE SYSTEM AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. CYNCEALTH DISCLAIMS ANY AND ALL RESPONSIBILITIES FOR ANY ACT OR OMISSION TAKEN OR MADE BY PARTICIPANT IN RELIANCE ON THE SYSTEM OR THE INFORMATION IN THE SYSTEM, INCLUDING INACCURATE OR INCOMPLETE INFORMATION. EXCEPT FOR CYNCEALTH'S INTELLECTUAL PROPERTY INFRINGEMENT INDEMNITY OBLIGATIONS HEREUNDER, EITHER PARTY'S BREACH OF THE CONFIDENTIALITY OBLIGATIONS OR VIOLATION OF APPLICABLE LAW, IT IS EXPRESSLY AGREED THAT IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL, INDIRECT,

CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUES, LOSS OF USE, OR LOSS OF INFORMATION OR DATA, WHETHER A CLAIM FOR ANY SUCH LIABILITY OR DAMAGES IS PREMISED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER THEORIES OF LIABILITY, EVEN IF SUCH PARTY HAS BEEN APPRISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES OCCURRING. CYNCHHEALTH DISCLAIMS ANY AND ALL LIABILITY FOR ERRONEOUS TRANSMISSIONS AND LOSS OF SERVICE RESULTING FROM COMMUNICATION FAILURES BY CARRIER LINES, TELECOMMUNICATION SERVICE PROVIDERS OR THE SYSTEM.

11.4 Unauthorized Access; Lost or Corrupt Data. CyncHealth IS NOT RESPONSIBLE FOR UNAUTHORIZED ACCESS TO PARTICIPANT'S TRANSMISSION FACILITIES OR EQUIPMENT BY INDIVIDUALS OR ENTITIES USING THE SYSTEM OR FOR UNAUTHORIZED ACCESS TO, OR ALTERATION, THEFT, OR DESTRUCTION OF PARTICIPANT'S DATA FILES, PROGRAMS, PROCEDURES, OR INFORMATION THROUGH THE SYSTEM. PARTICIPANT IS SOLELY RESPONSIBLE FOR VALIDATING THE ACCURACY OF ALL OUTPUT AND REPORTS OBTAINED THROUGH USE OF THE SYSTEM AND IS RESPONSIBLE FOR MAKING REASONABLE EFFORTS TO PROTECT PARTICIPANT'S OWN DATA AND PROGRAMS FROM LOSS BY IMPLEMENTING APPROPRIATE SECURITY MEASURES, INCLUDING ROUTINE BACKUP PROCEDURES. PARTICIPANT HEREBY WAIVES ANY DAMAGES OCCASIONED BY LOST OR CORRUPT DATA, INCORRECT REPORTS, OR INCORRECT DATA FILES RESULTING FROM PROGRAMMING ERROR, OPERATOR ERROR, OR EQUIPMENT OR SOFTWARE MALFUNCTION. CyncHealth IS NOT RESPONSIBLE FOR THE CONTENT OF ANY INFORMATION TRANSMITTED OR RECEIVED THROUGH CYNCHHEALTH'S PROVISION OF THE SERVICES.

11.5 Limitation of Liability. Each party shall be self-insured and/or procure and maintain insurance policies with such coverages and in such amounts and for such period of time as required by and set forth in Section 12 below. TO THE FULLEST EXTENT PERMITTED BY LAW, A PARTY'S TOTAL LIABILITY TO THE OTHER PARTY FOR ANY AND ALL INJURIES, CLAIMS, LOSSES, EXPENSES OR DAMAGES WHATSOEVER ARISING OUT OF, OR IN ANY WAY RELATED TO, THIS AGREEMENT FROM ANY CAUSE OR CAUSES INCLUDING BUT NOT LIMITED TO NEGLIGENCE, ERRORS, OMISSIONS, STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY (HEREAFTER A "CLAIM") SHALL NOT EXCEED THE SUM PAID ON BEHALF OF, OR TO THE LIABLE PARTY, BY ITS INSURERS IN SETTLEMENT OR SATISFACTION OF A CLAIM. IF NO SUCH INSURANCE COVERAGE IS PROVIDED WITH RESPECT TO A CLAIM, THEN THE LIABLE PARTY'S TOTAL LIABILITY FOR SUCH CLAIM SHALL NOT EXCEED AN AMOUNT EQUAL TO THE AGGREGATE FEES

ACTUALLY PAID BY PARTICIPANT UNDER THIS AGREEMENT FOR THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT FIRST GIVING RISE TO THE CLAIM OR FIVE HUNDRED THOUSAND DOLLARS (\$500,000), WHICHEVER IS GREATER. These provisions are not intended to waive a Party's sovereign immunity. Each Party's liability is governed by and limited to the extent provided by the Nebraska Political Subdivisions Tort Claims Act, or other applicable provisions of law.

11.6 Intellectual Property Indemnity. CyncHealth shall indemnify and hold Participant and its successors, officers, employees, and agents harmless from and against any and all claims, losses, damages, liabilities, judgments, awards, costs, and expenses (including legal fees) resulting from or arising out of any breach of the intellectual property representations and warranties made by CyncHealth, or which is based on a claim of an Infringement and CyncHealth shall defend and settle, at its expense, all suits or proceedings arising therefrom. Participant shall inform CyncHealth of any such suit or proceeding against Participant and shall have the right to participate in the defense of any such suit or proceeding at its expense. CyncHealth shall notify Participant of any actions, claims, or suits against CyncHealth based on an alleged Infringement of any Party's intellectual property rights in and to the System.

In the event an injunction is sought or obtained against use of the System and/or components thereof or in Participant's opinion is likely to be sought or obtained, CyncHealth shall promptly, at its option and expense, either:

- (a) Procure for Participant's end users the right to continue to use the infringing portion(s) of the System and/or component thereof as set forth in the Agreement; or,
- (b) Replace or modify the infringing portions of the System to make its use non-infringing while being capable of performing the same function without degradation of performance.
- (c) Additional Remedies. In the event that the Service, or any portion thereof, is held by a court of competent jurisdiction to infringe or constitute the wrongful use of any third party's proprietary rights and Authorized Users' right to use the Services is enjoined, or if CyncHealth in the reasonable exercise of its discretion instructs an Authorized User to cease using such Service in order to mitigate potential damages arising from a third party's claim of infringement or misappropriation, the Authorized User shall cease using such Services. In addition to CyncHealth's obligations under Section 11.6 , upon Participant's request, CyncHealth shall immediately perform one of the following as selected by CyncHealth: (i) replace the Services, with equally suitable and functionally equivalent non-infringing Services; (ii) modify the Services so that they are equally suitable and functionally equivalent to the



alleged infringing Service and its use by Authorized Users ceases to be infringing or wrongful; or (iii) procure for Authorized Users the right to continue using the services.

(d) Limitation. Notwithstanding the terms of Sections 11.6, CyncHealth will have no liability for an infringement or misappropriation claim to the extent that it is proximately caused by: (i) modifications to the Services or System made by a party other than CyncHealth, if a claim would not have occurred but for such modifications and such modifications were not authorized by this Agreement; (ii) the combination, operation or use of the Services or System with equipment, devices, software or data not supplied or recommended by CyncHealth, if a claim would not have occurred but for such combination, operation or use; (iii) Authorized Users' use of the Services of System other than in accordance with this Agreement and the Documentation; or, (iv) any Third-party Software or Third-party Services.

(e) Third-Party Software and Services. CyncHealth will cooperate with IP Indemnitee to pass through to IP Indemnitee any applicable indemnity received from a vendor of Third-party Software or Services included in the System of Services.

(f) Exclusive Remedy. SECTION 11.6 SETS FORTH THE ENTIRE LIABILITY AND OBLIGATION OF CYNCEALTH, AND PARTICIPANT'S EXCLUSIVE REMEDY AGAINST CYNCEALTH, WITH RESPECT TO ANY INTELLECTUAL PROPERTY INFRINGEMENT.

## 12. Insurance.

12.1 Participant Insurance. Participant shall be self-insured and/or obtain and maintain such policies of general liability, errors and omissions, and professional liability insurance with reputable insurance companies as required by the Policies and Procedures. This provision is not intended to waive a Party's sovereign immunity. Notwithstanding the requirements of this provision, each Party's liability is governed by and limited to the extent provided by the Nebraska Political Subdivisions Tort Claims Act, or other applicable provisions of law, and no Party shall be required to obtain insurance coverage for claims shielded by such.

12.2 CyncHealth Insurance. CyncHealth shall purchase and maintain, at all times that services are being performed under this Agreement, professional and general liability insurance with limits of not less than One Million Dollars (\$1,000,000) per occurrence and Three Million Dollars (\$3,000,000) in the aggregate per policy year through responsible insurance companies authorized to do business in Nebraska, or through a combination of insurance and self-insurance approved by Participant. Each party shall provide and

maintain workers' compensation insurance in the statutory amounts. At the request of Participant, CyncHealth may provide Participant with a certificate of insurance.

### **13. Term; Modification; Suspension; Termination.**

13.1 Term. The initial term of this Agreement shall commence on the Effective Date and continue for a period of one (1) year, and thereafter shall renew for successive one-year renewal terms until terminated as provided in this Section.

13.2 Termination upon Notice. CyncHealth or Participant may terminate this Agreement at any time without cause upon ninety (90) days prior written notice to the other Party.

13.3 Modification. CyncHealth may change the terms under which the System is provided to Participant (including terms set forth in this Agreement) by providing Participant not less than ninety (90) days' notice. Upon receipt of such a notice, Participant may terminate this Agreement by giving written notice to CyncHealth on or before the effective date of the change. Participant agrees that Participant's failure to give notice of termination prior to the effective date of the change constitutes acceptance of the change, which shall thereupon become part of this Agreement.

13.4 Termination, Suspension, or Amendment as a Result of Government Regulation. Notwithstanding anything to the contrary in this Agreement, either party shall have the right, on notice to the other Party, to immediately terminate or suspend this Agreement without liability:

- (a) To comply with any order issued or proposed to be issued by any governmental agency;
- (b) To comply with any provision of law, any standard of participation in any reimbursement program, or any accreditation standard; or,
- (c) If performance of any term of this Agreement by either party would cause it to be in violation of law, or would jeopardize its tax-exempt status.

### 13.5 Obligations After Termination.

- (a) Upon termination of this Agreement or any Attachment, Participant shall cease to use the System and CyncHealth will terminate Participant's access to the System. Participant will have thirty (30) days from the date of termination to pay CyncHealth the fees for the balance of the Term for any terminated portion of this Agreement.

(b) All the provisions of Section 10, Confidential Information; Section 11, Warranty, Disclaimer and Limitation of Liability; and Section 13.5, Obligations after Termination, shall survive the termination of this Agreement. In addition, where the terms of this Agreement or any Attachment specify that certain provisions will survive termination under certain conditions, those provisions shall survive under the applicable conditions.

**14. Dispute Resolution.** CyncHealth and Participant understand and agree that the implementation of this Agreement will be enhanced by the timely and open resolution of any disputes or disagreements between such Parties for the mutual benefit of both parties.

14.1 Each party hereto agrees to use its best efforts to cause any disputes or disagreements between such Parties to be considered, negotiated in good faith, and resolved as soon as possible.

14.2 In the event that any dispute or disagreement between the Parties cannot be resolved to the satisfaction of CyncHealth's project manager and Participant's project manager within ten (10) days after either such project manager has notified the other in writing of the need to resolve the specific dispute or disagreement within such ten (10) day period, then the dispute or disagreement shall be immediately referred in writing to the respective senior officers of Participant and CyncHealth for consideration.

14.3 No resolution or attempted resolution of any dispute or disagreement pursuant to this Article shall be deemed to be a waiver of any term or provision of this Agreement or consent to any breach or default unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented.

**15. Applicable Law.** The interpretation of this Agreement and the resolution of any disputes arising under this Agreement shall be governed by the laws of the State of Nebraska. If any action or other proceeding is brought on or in connection with this Agreement, the venue of such action shall be exclusively in Douglas County, Nebraska.

**16. Legal Compliance.** The Parties shall comply with all applicable state and federal laws relating to the provision of their respective services.

**17. No Assignment.** This Agreement may not be assigned or transferred by a Party without the prior written consent of the other Party.

**18. Supervening Circumstances.** No party to this Agreement shall be deemed in violation of this Agreement if it is prevented from performing any of the obligations under this Agreement by reason of severe weather and storms, earthquakes or other natural occurrences, strikes or other labor unrest, power failures, nuclear or other civil or military emergencies, acts of legislative,

judicial, executive, or administrative authorities, or any other circumstances that are not within its reasonable control.

**19. Severability.** Any provision of this Agreement that shall prove to be invalid, void, or illegal, shall in no way affect, impair, or invalidate any other provision of this Agreement, and such other provisions shall remain in full force and effect.

**20. Notices.** All notices required or permitted under this Agreement shall be in writing and sent by United States mail, fax transmission, or electronic mail.

**21. Waiver.** No term of this Agreement shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of a breach by the other, whether expressed or implied, shall not constitute a consent to, waiver of, or excuse for any other different or subsequent breach.

**22. Complete Understanding.** This Agreement contains the entire understanding of the Parties, and there are no other written or oral understandings or promises between the Parties with respect to the subject matter of this Agreement other than those contained or referenced in this Agreement. All modifications or amendments to this Agreement shall be made in in writing and signed by both Parties.

**23. Signature Authority.** The individuals executing this represent and warrant that they are competent and capable of entering into a binding contract, and that they are authorized to execute this Agreement on behalf of the Parties.

**24. No Medicare Exclusion.** The Parties hereby represent and warrant that they are not and at no time have been excluded from participation in any federally-funded health care program, including Medicare and Medicaid. Each Party hereby agrees to immediately notify the other Party of any threatened, proposed, or actual exclusion from federally-funded health care program, including Medicare or Medicaid. In the event that either Party is excluded from any federally-funded health care program during the term of this Agreement, or if at any time after the Effective Date of this Agreement, it is determined that either Party is in breach of this Article, this Agreement shall, as of the effective date of such exclusion or breach, automatically terminate.

**25. Rules of Construction.** Words used herein, regardless of the number used, shall be deemed and construed to include any other number, singular or plural, as the context requires, and, as used herein, unless the context requires otherwise, the words “hereof”, “herein”, and “hereunder” and words of similar import shall refer to this Agreement as a whole and not to any particular provision of this Agreement.

25.1 A reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or reenacted.

25.2 The term “including” shall be deemed to mean “including without limitation.”

25.3 Article and section headings used in this Agreement are for convenience of reference only and shall not affect the interpretation of this Agreement.

25.4 This Agreement is among sophisticated and knowledgeable Parties and is entered into by the Parties in reliance upon the economic and legal bargains contained herein and shall be interpreted and construed in a fair and impartial manner without regard to such factors as the Party who prepared, or caused the preparation of, this Agreement or the relative bargaining power of the Parties.

[SIGNATURES ON FOLLOWING PAGE]

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed in duplicate original as of the date(s) indicated below:

**Participant Name**

Name: Signatory Name

Title: Signatory Title

Address: Address

Phone: Phone Number

Email: Signatory Email Address

Signature: SIGNATURE AREA

**NEBRASKA HEALTH INFORMATION INITIATIVE, INC., dba CYNCHALTH**

Name: Jaime Bland

Title: President & CEO

Address: 11412 Centennial Road  
Suite 800  
La Vista, NE 68128

Phone: (402) 506-9900

Email: [jbland@cynchealth.org](mailto:jbland@cynchealth.org)

Signature: SIGNATURE AREA

### **Attachment 1: Services**

CyncHealth will provide the following to Participant and/or Users:

- Access to the System as described in Attachment 2 of this Agreement
- A training session for each User that will be offered multiple times to keep disruption to a minimum
- Access to education related to the use and access to systems
- Help desk access for application question service and system questions and resolving any identified issues related to services and systems

## Attachment 2: System

### HealthShare/Clinical Viewer

InterSystems HealthShare is the health information exchange (“HIE”) framework that brings together clinical information from multiple entities and sources quickly and accurately into a single view. This application offers simple access to patient clinical information for sharing and reporting purposes

The clinical viewer within the system provides an aggregated view of a patient’s clinical data based on information sent to the exchange from HL7v2 messages or HL7v3 documents. Reliable patient identification provides users with the ability to query for a patient’s records when parts of the continuum of care record are scattered across the community. This functionality includes searchable patient records from connected data sources within and without the HIE. Patient privacy is safeguarded to protect health information. Consent settings allow a patient to determine whether a medical professional should have access to their health information.

### Prescription Drug Monitoring Program

The enhanced Nebraska Prescription Drug Monitoring Program (“PDMP”) is a tool that collects dispensed controlled substance prescription information. Beginning in 2018, all prescriptions must be reported. This functionality is currently available to all prescribers and dispensers at no cost. This program is intended to prevent the misuse of controlled substances that are prescribed, allow prescribers and dispensers to monitor the care and treatment of patients, and enhance patient safety by prevention of adverse drug events (“ADEs”) through unintended medication discrepancies.

### Secured Direct Messaging

SES Direct is CyncHealth’s Health Information Services Provider. SES Direct is fully accredited and includes end to end message encryption which is a secure email service that allows providers to securely send and receive email messages and attachments containing a patient’s clinical data. Direct email addresses are utilized to enable interoperability and create access in the healthcare ecosystem using the Directory Services for inside network and outside.

### Unite Nebraska/SDOH platform

Unite Nebraska is a statewide coordinated care network designed to address social determinants of health. Partners in the network are connected through a shared technology platform, Unite Us, which enables them to send and receive electronic referrals, address patient’s social needs, and improve health across communities. Unite Us is a Business Associate to Covered Entities under HIPAA, follows the Health and Human Services (HHS) guidelines on Breach Notification and Breach Enforcement procedures established in the Health Information Technology for Economic and Clinical Health Act (HITECH 2009), and has implemented extensive standards to apply cross-functionality to Family Educational Rights Privacy Act (FERPA 1974) and Federal Information Processing Standards (FIPS) compliance.





Unite Us is securely managed on HIPAA compliant servers in a leading high-density data center with SAS-70 Type II certifications and includes safeguards such as 24-7 video surveillance, physical locks and structured access controls. Additionally, Unite Us has signed a Business Association Agreement (BAA) with CyncHealth as well as with all third-party technical partners.

### Attachment 3: DURSA Mandated Flow-Down Provisions

These additional flow-down provisions relate to the exchange of Message Content (as defined below) in accordance with the Data Use and Reciprocal Support Agreement (the “DURSA”) entered into by CyncHealth. To the extent of a conflict between these provisions and the Agreement, these provisions shall govern with respect to the exchange of Message Content in accordance with the DURSA. These provisions are subject to change in accordance with requirements of the DURSA.

**1. Definitions.** Capitalized terms used but not otherwise defined in the Agreement or this Attachment shall have the meaning ascribed in HIPAA.

1.1 “Applicable Law” means:

(a) for the Participants that are not Federal Participants, all applicable statutes and regulations of the State(s) or jurisdiction(s) in which the Participant operates, as well as all applicable Federal statutes, regulations, standards and policy requirements;

(b) for the federal Participants, all applicable Federal statutes, regulations, standards and policy requirements.

1.2 “Message Content” means Participant’s Shared Information, Protected Health Information, de-identified data, individually identifiable information, pseudonymized data, metadata, and schema.

1.3 “Permitted Purpose” means one of the following reasons for which Participant or its Authorized Users may legitimately Transact Message Content:

(a) Treatment, Payment, Health Care Operations, and Authorization based disclosures as defined by HIPAA;

(b) Transaction of Message Content related to value-based payment models, alternative payment arrangements or financial risk sharing models of any nature whether for Medicare, Medicaid, other federal programs, commercial payers or employer self-insured arrangements. This could include, but is not limited to, participation in Medicare bundled payments, the Medicare Shared Savings Program, other Medicare Alternate Payment programs, Medicaid Managed Care programs or commercial value-based payment programs;

(c) Transaction of Message Content for certain specialized government functions which are necessary to fulfill an agency’s statutory obligations for programs the

agency administers including, but not limited to: (i) activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission; (ii) for the purpose of the Department of Veterans Affairs determining the individual's eligibility or entitlement to benefits under the VA upon separation or discharge of the individual from military service; (iii) to determine eligibility for or entitlement to or provision of other government benefits; (iv) for activities related to eligibility for or enrollment in a health plan that is a government program; (v) for administering a government program providing public benefits, to coordinate covered functions; or, (vi) to improve administration and management relating to the covered functions of such government programs;

(d) Public health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514I;

(e) Any purpose to demonstrate meaningful use of certified electronic health record technology by the (i) Submitter, (ii) Recipient or (iii) Covered Entity on whose behalf the Submitter or the Recipient may properly Transact Message Content under this Agreement, provided that the purpose is not otherwise described in subsections 1-46 of this definition and the purpose is permitted by Applicable Law, including but not limited to the HIPAA Regulations. "Meaningful use of certified electronic health record technology" shall have the meaning assigned to it in the regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102;

(f) Transaction of Message Content in support of an individual's: (i) right to access their health information or (ii) right to direct with whom their information can be shared or where their information should be sent. For the avoidance of doubt, a Participant may be prevented from disclosing information due to Applicable Law even though the individual asserts this Permitted Purpose;

1.4 "Transact" means to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content. While Transacting Message Content in accordance with the DURSA, Participant shall:

(a) Comply with all Applicable Law;

(b) Reasonably cooperate with CyncHealth on issues related to the Agreement and the DURSA;

(c) Transact Message Content only for a Permitted Purpose;

(d) Use Message Content received from another Participant or Authorized User in accordance with the terms and conditions of the Agreement and the DURSA;

(e) As soon as reasonably practicable after determining that a Breach occurred, report such Breach to CyncHealth; and,

(f) Refrain from disclosing to any other person any passwords or other security measures issued to the Authorized User by the Participant.

**2. Compliance and Cooperation.** Participants agree to comply with all applicable law and to reasonably cooperate with issues related to DURSA. See Section 3.2(b) of Agreement regarding compliance with applicable law and Sections 3.4(b), 3.6. 3.7(b)(vi), and 3.8 of Agreement regarding cooperation.

**3. System Access Policies.** For System Access Policies as agreed to in DURSA, please see Section 2 of the Agreement which includes guidelines for Permitted Uses (3.1), Prohibited Uses (3.2), Participant's systems requirements(3.3), required safeguards (3.5), and notification of CyncHealth in the case of a security breach (3.5(d)).

3.1. Identification & Authentication. Participant shall employ a process by which the Participant, or its designee, uses credentials to verify the identity of each Participant User and uses reasonable security measures to ensure the protection of confidential information.

#### **Attachment 4: Unite Us Platform**

These additional provisions relate to the Unite Us Platform in accordance with the agreement between Unite Us and CyncHealth. To the extent of a conflict between these provisions and the Agreement, these provisions shall govern with respect to the Unite Us Platform. These provisions are subject to change in accordance with requirements of the Unite Us Platform.

#### **1. Definitions**

1.1 “Network” shall mean the network created by the Unite Us platform that connects health and social service organizations.

1.2 “Network Participant” shall mean any health and social service organization that connects clients with services using the Unite Us Platform

1.3 “Network Participant Data” means information (including, without limitation, PII provided to Network Participant by or at the direction of a client or information Network Participant requires to provide and document services to such client within the Unite Us Platform in the course of the Network Participant’s use of the Network.

1.4 “Authorized User” shall mean individuals associated with or employed by a Network Participant that such participant has authorized to access the Unite Us Platform.

#### **2. While connected to the Network, Network Participant shall:**

2.1 Make a reasonable effort to keep an up-to-day profile within the Unite Us Platform by regularly updating available programs, eligibility for such programs, and appropriate contact information for processing of assistance requests and referrals;

2.2 Be responsible for the acts or omissions of any person who accesses the Unite Us Platform using passwords or access procedures provided to or created by Network Participant or its Authorized User. Unite Us reserves the right to refuse registration of, or to cancel, login IDs that violate these Network Terms;

2.3 Notify Unite Us immediately upon learning of any unauthorized use of Network Participant’s or any of its Authorized Users’ accounts;

2.4 Require each Authorized User accessing the Unite Us Platform to enter electronically into an end-user license agreement governing access to, use of, and all rights and obligations of the end-user relating to the Unite Us Platform; and,

2.5 Immediately terminate access to the Unite Us Platform of any Authorized User who is no longer associated with or employed by such Network Participant or shall contact Unite Us to terminate such access.

**3. Hardware and Connectivity.** Network Participant shall be solely responsible for all hardware and Internet connectivity required to access the Network and shall use supported Internet browsers to access the Unite Us Platform.

**4. License to the Unite Us Platform.** Unite Us hereby grants to Network Participant a non-exclusive, non-transferable license to (a) access and use the Unite Us Platform for the benefit of Network Participant; (b) reproduce, distribute and display the documentation provided by Unite Us solely to its Authorized Users; and (c) use and access any Network Participant Data as necessary for the care and treatment of individuals seeking treatment or services from Network Participant in compliance with HIPAA and other applicable privacy laws.

**5. Restrictions.** Network Participant may not and may not permit third parties to (a) sell, assign, sublicense or otherwise transfer the Unite Us Platform to third parties; (b) resell the Unite Us Platform to any third party; (c) use the Unite Us Platform to provide or perform service bureau processing, or hosting services for any third party; (d) otherwise use the Unite Us Platform for the benefit of any third party; (e) disassemble, decompile, reverse engineer or use any other means to attempt to discover any source code of the Unite Us Platform, or the underlying ideas, algorithms or trade secrets therein; (f) use the Unite Us Platform to knowingly transmit malware, spam or other unsolicited emails in violation of applicable law, or to post or send any unlawful, threatening, harassing, racist, abusive, libelous, pornographic, defamatory, obscene, or other similarly inappropriate content; (g) remove any copyright notice, trademark notice or other proprietary legend set forth on or contained within any of the documentation or other materials provided by Unite Us; or (h) otherwise use the Unite Us Platform or Network Participant Data in violation of any applicable law.

**6. Data.** Participation in the Network requires Participants to grant all other Network Participants and their Authorized Users an irrevocable, worldwide, non-exclusive, royalty-free, fully paid-up license to access the Network Participant Data as is permitted for the Unite Us Platform to function. All use of such Network Participant data must conform to all applicable laws. In addition, Network Participants grant Unite Us an irrevocable, worldwide, non-exclusive, royalty-free, fully paid-up license to use, reproduce, modify, distribute and display Network Participant Data (i) on the Unite Us Platform, and (ii) for Network evaluation.

6.1 Data Ownership. Each Network Participant shall remain the owner of any Network Participant Data inputted by such Network Participant of all individuals registered with a Network Participant and nothing here in is intended or will be deemed in any way to limit a Network Participant's use of its own Network Participant Data outside of the Unite Us Platform.

6.2 Data Restrictions. Network Participant may include personally identifiable data (including protected health information) (collectively, “ PII ”) in Network Participant Data and provide PII to Unite Us in the course of using the Unite Us Platform only if (a) disclosure of such PII is necessary for Network Participant’s exploitation of the Unite Us Platform and services provided by Unite Us; (b) Network Participant has all consents, rights and authorizations under applicable law necessary to provide Unite Us with the Network Participant Data hereunder; (c) such PII is collected by Network Participant and disclosed to Unite Us pursuant to and in accordance with Network Participant’s applicable privacy policies and (d) Network Participant’s provision of such PII to Unite Us and Unite Us’ retention and use of such PII as contemplated under these Network Terms does not and will not violate any applicable Network Participant privacy policy or any applicable laws.

### **Attachment 5: InterSystems Mandated Flow-Down Provisions**

These additional flow-down provisions relate to the technology and services provided by InterSystems HealthShare (ISC). To the extent of a conflict between these provisions and the Agreement, these provisions shall govern with respect to the technology and services provided by ISC. These provisions are subject to change in accordance with requirements of ISC.

1. The ISC System (as more specifically described on Attachment 2) may be used only by Authorized Users for whom all applicable fees have been paid.
2. Participant shall maintain the confidentiality of the ISC System.
3. Participant shall not use the ISC System for any purpose outside the scope of the Agreement. Participant shall not reverse engineer, disassemble or decompile the ISC System. Participant shall not duplicate the ISC System.
4. Participant is responsible to ensure Participant and its Authorized Users do not:
  - 4.1 In connection with any ISC System, send or store infringing, obscene, threatening, or otherwise unlawful or tortious material, or otherwise use the ISC System to violate privacy rights;
  - 4.2 Send or store malicious code in connection with the ISC System; or
  - 4.3 Interfere with or disrupt performance of the ISC System or the data contained therein; or
5. Participant is responsible for auditing and keeping current all Authorized User account access to the ISC System. Participant shall be responsible for establishing a process to communicate patient opt-outs in accordance with the Policies and Procedures and Applicable Law.
6. Participant shall be responsible for its data entry activities, and for the accuracy of any raw Participant's Shared Information delivered to the System. ISC shall not be responsible for errors in raw Participant's Shared Information or data entry done by Participant, or for errors in services, programs, hardware, data files, or output ISC provides to or maintains, if those ISC errors result from errors in the input data.
  - 6.1 Participant and its Authorized Users shall not:



- (a) modify or copy the ISC System or any documentation made available in connection with the ISC System or create any derivative works based on the ISC System;
- (b) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share, offer in a service bureau, or otherwise make the Solution available to any third party, other than as permitted herein;
- (c) access the ISC System other than as permitted in the Agreement;
- (d) copy any features, functions, integrations, interfaces or graphics of the ISC System; or use the ISC System in violation of applicable Laws.

**Attachment 6: Fees**

There is no cost to share your data to CyncHealth or have access to the PDMP. The annual HIE participation fee will be billed quarterly. Partial year participation billings will begin when full ADT connection is completed or Participant receives access to the System, whichever occurs first. Annual participation fee is subject to change each calendar year, as the pricing schedule is approved by the CyncHealth Board of Directors annually.

**ANNUAL CYNCHHEALTH FEES**

Sharing data & PDMP Access	\$0.00
CyncHealth Annual Participant Fee for 2022	\$Participant Fees*
<b>TOTAL</b>	<b>\$Participant Fees</b>

\*Annual fee quoted will be pro-rated and charged only for the months of access during 2022

## Attachment 7: Business Associate Agreement

**THIS BUSINESS ASSOCIATE AGREEMENT** (“BAA”) amends and is made a part of all Services Agreements (as defined below) between Nebraska Health Information Initiative, Inc., DBA CyncHealth (“Business Associate”) and Participant Name (“Participant” or “Covered Entity”) (collectively, the “Parties”), as of the date of last signature below. This Agreement supersedes and replaces all prior Business Associate Agreements or Amendments between the parties.

### 1. **Definitions.**

a. **Catch-all definition.** The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclose or Disclosure, Electronic Protected Health Information, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information or PHI, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Other capitalized terms used but not otherwise defined in this Agreement shall have the meaning ascribed in the HIPAA Rules.

b. **Specific definitions.**

1. **“Business Associate”** shall generally have the same meaning as the term “Business Associate” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean the party identified above as Business Associate.
2. **“Business Associate Functions”** means all functions performed by Business Associate under one or more Services Agreements on behalf of Covered Entity which involve the creation, receipt, maintenance or transmission of PHI by Business Associate or its agents or Subcontractors on behalf of Covered Entity.
3. **“Covered Entity”** shall generally have the same meaning as the term “Covered Entity” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean the party identified above as Covered Entity.
4. **“HIPAA Rules”** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended at the time the section is to be applied.
5. **“Qualified Service Organization”** shall have the same meaning as the term “Qualified Service Organization” in 42 C.F.R. § 2.11.
6. **“Services Agreements”** means all agreements whether now in effect or hereafter entered into, between Covered Entity and Business Associate for the performance of Business Associate Functions by Business Associate.

2. **Purpose.** Covered Entity is a covered entity under HIPAA and CyncHealth, Inc. is its Business Associate. HIPAA requires Covered Entity to obtain satisfactory written

contractual assurances from its business associates before furnishing them with PHI or permitting them to obtain or create PHI to perform business associate functions. This Agreement is entered into to provide Covered Entity with the contractual assurances required under HIPAA. This BAA is made part of, and subject to the terms and conditions of, each Services Agreements. This Agreement and the Services Agreements shall be construed wherever reasonable as being consistent with each other. When such construction is unreasonable, the terms of this Agreement shall take precedence. In addition, in the case that the Covered Entity operates a federally assisted program that requires compliance with the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law and regulations, 42 U.S.C § 290dd-2 and 42 C.F.R Part 2 (collectively "Part 2"), Business Associate is also a Qualified Service Organization ("QSO") under Part 2 and agrees to certain mandatory provisions regarding the disclosure of substance abuse treatment information.

3. **Obligations of Business Associate.** As an express condition of performing Business Associate Functions, Business Associate agrees to:
- a. Not Use or Disclose PHI other than as permitted or required by this Agreement or as otherwise Required by Law.
  - b. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information, to prevent Use or Disclosure of PHI other than as provided for in this Agreement.
  - c. Report to Covered Entity's designated privacy official, without unreasonable delay but in no event more than three (3) business days after discovery by Business Associate, any Use or Disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware, including any Breach of Unsecured Protected Health Information as required at 45 CFR 164.410, and any Security Incident of which it becomes aware, together with any remedial or mitigating action taken or proposed to be taken with respect thereto. If Business Associate does not have available complete information in satisfaction of 45 CFR 164.410(c) within three (3) business days of discovery of the impermissible Use or Disclosure, Business Associate shall provide all information it has at such time, and immediately update Covered Entity with additional information as it becomes available through prompt investigation. This BAA serves as Business Associate's notice to Covered Entity that attempted but unsuccessful Security Incidents regularly occur and that no further notice will be made by Business Associate unless there has been a successful Security Incident or attempts or patterns of attempts that Business Associate determines to be suspicious. Business Associate shall cooperate with Covered Entity in mitigating, at its sole expense, any harmful effects of any impermissible Use or Disclosure.
  - d. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree in writing to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information.

- e. Within five (5) business days of request by an Individual or notification by Covered Entity, make available to Covered Entity the Individual's PHI maintained by Business Associate in a Designated Record Set in accordance with 45 CFR 164.524. If the requested PHI is maintained in one or more Designated Record Sets electronically and if the Individual requests an electronic copy of such PHI, Business Associate must provide Covered Entity with access to the PHI in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to between Covered Entity and the Individual and within the technical capability of Business Associate. Business Associate is not authorized to independently respond to an Individual's request and shall refer all Individuals to Covered Entity to make any such request.
- f. Notify Covered Entity within five (5) business days of any request by an Individual to amend PHI maintained by Business Associate in a Designated Record Set, direct the requesting Individual to Covered Entity for handling of such request, and promptly incorporate any amendment accepted by Covered Entity and communicated to Business Associate in accordance with 45 CFR 164.526. Business Associate is not authorized to independently agree to any amendment of PHI and shall direct all Individuals to Covered Entity to make any such request.
- g. Maintain a record of those Disclosures of PHI by Business Associate or its agents or Subcontractors which are subject to the Individual's right to an accounting under 45 CFR 164.528 and within five (5) business days of notification by Covered Entity report such Disclosures to Covered Entity in a form permitting Covered Entity to respond to an Individual's request for an accounting. Business Associate is not authorized to independently respond to an Individual's request and shall direct all Individuals to Covered Entity to make any such a request.
- h. Make its internal practices, books and records relating to this Agreement available to the Secretary of HHS and to Covered Entity for purposes of determining Covered Entity's and Business Associate's compliance with the HIPAA Rules.
- i. Comply with any voluntary restriction on Use or Disclosure of PHI under 45 CFR 164.522(a) of the HIPAA Rules when accepted by Covered Entity and communicated to Business Associate. Business Associate shall direct Individuals to Covered Entity to make any such request.
- j. Comply with any reasonable requests by Individuals under 45 CFR 164.522(b) to receive communications of PHI by alternative means or at alternate locations when accepted by Covered Entity and communicated to Business Associate. Business Associate shall direct Individuals to Covered Entity to make any such request.
- k. Limit the Uses and Disclosures of, or requests for, PHI for purposes described in this Agreement to the Minimum Necessary to perform the required Business Associate Function. Business Associate shall comply with any additional requirements for the determination of Minimum Necessary as are required from

time to time by the HIPAA Rules, as amended, or through additional guidance published by the Secretary.

- i. To the extent Business Associate is expressly obligated under the Services Agreements to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).
  - m. Except for the specific Uses and Disclosures for the Business Associate's own management and administration or to carry out the legal responsibilities of Business Associate, Business Associate shall not Use or Disclose PHI in a manner that would violate the HIPAA Rules if done by Covered Entity.
  - n. Business Associate shall not receive remuneration, either directly or indirectly in exchange for PHI, except as may be permitted by HIPAA.
  - o. Where applicable, Business Associate acknowledges that in receiving, storing, processing, or otherwise using any information from the alcohol/drug programs about the clients of a federally assisted program that requires compliance with Part 2, it is fully bound by the provisions of the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2.
4. **Permitted Uses and Disclosures of PHI.** Business Associate shall only Use or Disclose PHI as follows:
- a. Business Associate may Use or Disclose PHI as Required by Law.
  - b. Business Associate may Use or Disclose PHI as necessary to carry out Business Associate Functions.
  - c. Business Associate may Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.
  - d. Business Associate may Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the Disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that the information will remain confidential and be Used or further Disclosed only as Required by Law or for the purposes for which it was Disclosed to the person, and the person notifies Business Associate in writing of any instances of which it is aware in which the confidentiality of the information has been breached or compromised within three (3) business days of becoming aware of the occurrence.
  - e. Business Associate may provide Data Aggregation services relating to the Health Care Operations of Covered Entity.
  - f. Business Associate may Use PHI to de-identify the information in accordance with 45 CFR 164.514(a)-(c).
  - g. Business Associate will require any agent and/or subcontractors who may have access to PHI to agree to comply with 42 C.F.R. Part 2, and if Business Associate learns of a pattern or practice by the agent/subcontractor that is a material breach

of the contract with Business Associate, Business Associate will take reasonable steps to cure the breach or terminate the contract, if feasible.

5. **Responsibilities of Covered Entity.** Covered Entity agrees to:
  - a. Notify Business Associate promptly of any restriction on the Use or Disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent such restriction may affect Business Associate's Use or Disclosure of PHI.
  - b. Notify Business Associate of any changes in, or revocation of, the permission by an Individual to Use or Disclose PHI, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI.
  - c. Provide Business Associate with a copy of any amendment to PHI which is accepted by Covered Entity under 45 CFR 164.526 which Covered Entity believes will apply to PHI maintained by Business Associate in a Designated Record Set
  - d. Not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity, with exception for any Data Aggregation services permitted under Section 4.
  - e. Obtain any consent, authorization, or permission that may be required by the Privacy Rule, Part 2.
6. **Supervening Law.** Upon the enactment of any law or regulation affecting the Use or Disclosure of PHI, or the publication of any decision of a court of the United States or of this state relating to any such law, or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, the parties agree to amend this Agreement in such manner as is necessary to comply with such law or regulation. If the parties are unable to agree on an amendment within thirty (30) days, either party may terminate the Services Agreements on not less than thirty (30) days' written notice to the other.
7. **Term and Termination.**
  - a. **Term.** This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, including return or destruction of all PHI in Business Associate's possession (or in the possession of Business Associate's agents and Subcontractors), unless sooner terminated as provided herein. It is expressly agreed that the terms and conditions of this Agreement designed to safeguard PHI shall survive expiration or other termination of the Services Agreements and shall continue in effect until Business Associate has performed all obligations under this Agreement and has either returned or destroyed all PHI.
  - b. **Termination.** Covered Entity may immediately terminate this Agreement and the Services Agreements, if Covered Entity makes the determination that Business Associate has breached a material term of this Agreement. Alternatively, Covered Entity may choose to provide Business Associate with written notice of the existence of an alleged material breach, and afford Business Associate an opportunity to cure the alleged material breach upon mutually agreeable

terms. Failure to take reasonable steps to cure the breach is grounds for the immediate termination of this Agreement.

- c. **Business Associate Obligations Upon Termination.** Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:
  - i. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities or as to which Business Associate reasonably determines such PHI is technically incapable of being returned or destroyed;
  - ii. Return to Covered Entity or, if not provided for in the Services Agreements, destroy the PHI not retained pursuant to Section 8.c.(i) that the Business Associate maintains in any form;
  - iii. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information retained by Business Associate to prevent Use or Disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
  - iv. Not Use or Disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at Sections 4.c. and 4.d. which applied prior to termination; and,
  - v. Return to Covered Entity or, if not provided for in the Services Agreements, destroy the PHI retained by Business Associate pursuant to Section 8.c.(i) when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities, except where Business Associate reasonably determines such PHI is not technically capable of being returned or destroyed.
8. **Qualified Services Organization Agreement.** Where applicable, Covered Entity and Business Associate hereby agree that this Agreement constitutes a Qualified Service Organization Agreement ("QSOA") as required by 42 C.F.R. Part 2. Accordingly, information obtained by Business Associate relating to individuals who may have been diagnosed as needing, or who have received, substance use disorder treatment services shall be maintained and used only for the purposes intended under this Agreement and in conformity with all applicable provisions of 42 U.S.C. §290-dd-2 and the underlying federal regulations, 42 C.F.R. Part 2. This includes but is not limited to resisting any efforts in judicial proceedings to obtain access to the PHI, pursuant to 42 C.F.R. Part 2.
9. **Miscellaneous.**
  - a. **Covered Entity.** For purposes of this Agreement, and as applicable to the Business Associate Functions of Business Associate under the Services Agreements covered by this Agreement, references to Covered Entity shall include



- the named Covered Entity and all other covered entities named in and covered by the Services Agreements.
- b. Survival. The respective rights and obligations of Business Associate and Covered Entity hereunder shall survive termination of this Agreement according to the terms hereof and the obligations imposed on Covered Entity and Business Associate under the HIPAA Rules.
  - c. Interpretation; Agreement. This Agreement shall be interpreted and applied in a manner consistent with Covered Entity's and Business Associate's obligations under the HIPAA Rules, including Part 2. All amendments shall be in writing and signed by both parties, except that this Agreement shall attach to additional Services Agreements entered into between the parties in the future without the necessity of amending this Agreement each time. This Agreement is intended to cover the entire Business Associate *relationship* between the parties, as amended, from time to time, through Services Agreements or other means.
  - d. Waiver. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.
  - e. Severability. The invalidity or unenforceability of any provisions of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement.
  - f. Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.
10. Insurance. Business Associate agrees to maintain appropriate insurances levels as outlined in Section 12.2 of the Participation Agreement.

[SIGNATURES ON FOLLOWING PAGE]

**IN WITNESS WHEREOF**, each of the undersigned has caused this Agreement and all of its integrated Attachments included herein and added any time hereafter, to be duly executed in its name and on its behalf.

**Participant Name**

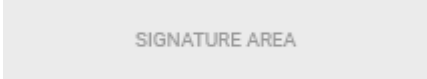
Name: Signatory Name

Title: Signatory Title

Address: Address

Phone: Phone Number

Email: Signatory Email Address

Signature: 

**NEBRASKA HEALTH INFORMATION INITIATIVE, INC., dba CYNCHALTH**

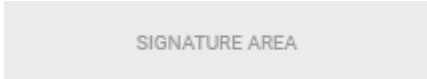
Name: Jaime Bland

Title: President & CEO

Address: 11412 Centennial Road  
Suite 800  
La Vista, NE 68128

Phone: (402) 506-9900

Email: jbland@cynchealth.org

Signature: 

**Attachment 8: Additional Authorized Facilities**

CyncHealth will provide access to the System for the additional facilities listed below (each an “Additional Authorized Facility”). Participant will pay the fees set forth in Attachment 7 of this Agreement.

Additional Authorized Facilities:

<b>Facility Name</b>	<b>Address</b>
Opportunity.Fac1_Legal_Name__c	Opportunity.Fac1_Address__c
Opportunity.Fac2_Legal_Name__c	Opportunity.Fac2_Address__c
Opportunity.Fac3_Legal_Name__c	Opportunity.Fac3_Address__c

Additional Facilities as a Participant

Additional Authorized Facilities will be considered a Participant for purposes of the Agreement, in addition to the Business Associate Agreement contained herein, and will be bound by such terms set forth therein.

**Attachment B**  
**Minnesota Privacy Policies**

**Minnesota privacy policies**

**Table of Contents**

**BREACH OF UNSECURED PHI**..... 1

**DISCLOSING INFORMATION TO BUSINESS ASSOCIATE SUBCONTRACTOR** ..... 4

**USING AND DISCLOSING OF HEALTH INFORMATION** ..... 1

HIPAA Authorization Checklist ..... 5

**DISCLOSURES FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS**..... 1

**MINIMUM NECESSARY FOR REQUESTS FOR, OR USES OR DISCLOSURES OF, PHI** ..... 2

**CONSENT TO DISCLOSE HEALTH INFORMATION UNDER MINNESOTA LAW** ..... 1

**EXCHANGING INFORMATION WITH OUT-OF-STATE PROVIDERS** ..... 1

**AUTHORIZED PURPOSES FOR REDISCLOSURE OF PART 2 DATA** ..... 2

Consumer Opt-Out Procedure ..... 6

    PROCEDURE ..... 6

Opt-Out Policy ..... 9

DEFINITIONS ..... 9

PURPOSE ..... 9

SCOPE AND APPLICABILITY ..... 10

ROLES AND RESPONSIBILITIES ..... 10

POLICY ..... 10

    Opt-Outs..... 10

    Request Process ..... 10

    Participant Communication..... 10

    Opt-Out Impact ..... 11

COMPLIANCE ..... 11

Objective ..... 15

Process ..... 15

    Position Requisitions..... 15

Position Postings.....	15
Internal Transfers.....	15
Interview Training.....	16
Interview Process.....	16
Staffing Agencies.....	16
Pre-Employment Screening.....	17
Offer.....	17
Contract Positions.....	17
Acknowledgment.....	17
Table of Contents.....	19
Tax Status and Purpose.....	21
Service Area.....	22
Division of Responsibilities.....	23
Chart of Accounts.....	23
Accounting Principles.....	23
Revenue Recognition.....	23
Matching of Revenues and Expenses.....	23
Fixed Assets and Depreciation.....	24
Donated Materials and Services.....	24
Data Cutoff.....	24
Cash Disbursements.....	25
Capital Acquisitions.....	25
Supplies, Services, and Other Invoices.....	25
Invoice Payment.....	26
Payroll.....	26
Expense Reimbursements.....	26
Cash/Check Receipts.....	27
Bank Reconciliations.....	27

End of Month Accounting ..... 28

End of Year Accounting ..... 28

Cost Allocations ..... 28

Investments ..... 28

Debt ..... 1

Reserves and Designated Funds ..... 1

Internal Controls and Financial Audit ..... 1

Credit Card Policy ..... 2

Compliance ..... 2

Budgeting ..... 3

Software Authorization and Backup ..... 3

Record Retention ..... 3

Maintenance of Accounting Policies Manual ..... 3

Preparation of Tax Returns ..... 4

Property and Equipment Inventory ..... 4

Grants and Contracts ..... 5

Revision Tracking ..... 5

<b>Document Group Title:</b> Minnesota Privacy Policies	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b>	<b>Approval Committee:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and contractors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
<b>Title</b>	<b>Title</b>	

**In General:** Any terms used but not otherwise defined in this policy have the definitions set forth in HIPAA Privacy Rule, HIPAA Security Rule and HIPAA Breach Notification Rule, 42 C.F.R. Part 2, or the Minnesota Health Records Act, as applicable. The following definitions have a meaning specific to these policies or, if the definitions are the same as the definitions provided in the applicable law, are provided for the convenience of the reader.

- 1) **Affiliate**: An entity that controls, is controlled by, or is under common control with another entity.
- 2) **Authorization**: A signed written document meeting the requirements of 45 C.F.R. § 164.508.
- 3) **Breach**: Except as otherwise provided in the HIPAA breach notification rule, “breach” means the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule which compromises the security or privacy of the protected health information.
- 4) **Consent**: Written permission to release health information that is dated and signed by the individual.
- 5) **Health Care Operations**: Any of the following activities, to the extent that the activities are related to covered functions:
  - (i) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
  - (ii) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-



health care professionals, accreditation, certification, licensing, or credentialing activities;

- (iii) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;
  - (iv) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
  - (v) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
  - (vi) Business management and general administrative activities of the entity, including, but not limited to:
    - (A) Management activities relating to implementation of and compliance with the requirements of this subchapter;
    - (B) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
    - (C) Resolution of internal grievances;
    - (D) The sale, transfer, merger, or consolidation of all or part of *CyncHealth* with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
    - (E) Consistent with the applicable requirements of § 164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of *CyncHealth*.
- 6) **HIPAA**: The federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and the accompanying Regulations.
- 7) **Medical Emergency**: Medically necessary care which is immediately needed to preserve life, prevent serious impairment to bodily functions, organs, or parts, or prevent placing the physical or mental health of the patient in serious jeopardy.
- 8) **Mental Health Records**: Information, whether oral or recorded, that relates to the past, present, or future mental health or condition of an individual.
- 9) **Minnesota Health Records Act**: Minnesota Statutes sections 144.291–144.298.
- 10) **Payment**: Payment means:
- (i) The activities undertaken by:

- (A) Except as prohibited under 45 CFR § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
  - (B) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
- (ii) The activities in section (i) of this definition relate to the individual to whom health care is provided and include, but are not limited to:
- (A) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
  - (B) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
  - (C) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
  - (D) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
  - (E) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
  - (F) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
    - (1) Name and address;
    - (2) Date of birth;
    - (3) Social security number;
    - (4) Payment history;
    - (5) Account number; and
    - (6) Name and address of the health care provider and/or health plan.

11) **PHI**: Protected health information as defined in 45 C.F.R. 160.103.

12) **Psychotherapy Notes**: Notes recorded (in any medium) by a health care 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.

13) **Qualified Service Organization**: An individual or entity who:

- (i) Provides services to a part 2 program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy, and
  - (ii) Has entered into a written agreement with a part 2 program under which that individual or entity:
    - (A) Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the part 2 program, it is fully bound by the Part 2 regulations; and
    - (B) If necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by the Part 2 regulations.
- 14) **Regulations:** the HIPAA Privacy Rule (“Privacy Rule”), HIPAA Security Rule (“Security Rule”), and the HIPAA Breach Notification Rule (“Breach Notification Rule”), which are codified in 45 C.F.R. Parts 160 and 164.
- 15) **Related Health Care Entity:** An Affiliate of the provider releasing the health records.
- 16) **Secretary:** The Secretary of the United States Department of Health and Human Services
- 17) **Substance Use Disorder:** A cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal. This definition does not include tobacco or caffeine use.
- 18) **Treating Provider Relationship:** Means that, regardless of whether there has been an actual in-person encounter:
  - (i) A patient is, agrees to, or is legally required to be diagnosed, evaluated, and/or treated, or agrees to accept consultation, for any condition by an individual or entity, and;
  - (ii) The individual or entity undertakes or agrees to undertake diagnosis, evaluation, and/or treatment of the patient, or consultation with the patient, for any condition.
- 19) **Treatment:** The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
- 20) **Withdrawal Management:** The use of pharmacotherapies to treat or attenuate the problematic signs and symptoms arising when heavy and/or prolonged substance use is reduced or discontinued

- 21) **Workforce**: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

**BREACH OF UNSECURED PHI**

<b>Document Group Title:</b> Minnesota Privacy Policies	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b>	<b>Approval Committee:</b>	<b>Referenced Procedures:</b> Incident Management Policy & Incident Management Procedures
<b>Intended Audience:</b> All CyncHealth staff and contractors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
<b>Title</b>	<b>Title</b>	

**I. Breach Policy:**

**A. Purpose**

CyncHealth must comply with rules related to privacy incident response and breach notification as a Business Associate to Participant Covered Entities. CyncHealth shall immediately respond to any actual or potential Breach of PHI (a “Privacy Incident”) to ensure confidentiality is maintained and to mitigate any adverse effects resulting from the Privacy Incident. Privacy Incidents shall be reported to the Privacy/Security Official immediately for further investigation as outlined below.

**B. In General**

The Privacy/Security Official shall notify affected Covered Entities according to the contractual obligations of the Business Associate Agreements after discovery of any use or disclosure of PHI not provided for by any Agreements of which CyncHealth becomes aware.

**1. Notification of Privacy/Security Official**

Workforce members shall as soon as possible, notify the Privacy/Security Official of any Privacy Incident. The Privacy/Security Official shall ensure that any necessary training occurs so that Workforce members understand their obligations to make such reports to the Privacy/Security Official. The Privacy/Security Official, will investigate all reports of Privacy Incidents and report such incidents in accordance with section 4 below and 45 CFR §164.410.

**3. Incident Assessment for Breach of a Security of the System according to Minn. Stat. § 325E.61**

- **Assessment to Determine Whether the Privacy Incident is a Breach of the Security of the System**

- Following notification of Privacy/Security Official of any Privacy Incident, the Privacy/Security Official, along with the Response Team, will investigate and determine whether the Privacy Incident constitutes a breach of the security of the system as defined in Minnesota Statutes section 325E.61.
- **Definition of Breach of the Security of the System**
  - “Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by *CyncHealth*.
- **Exception**
  - Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
- **Definition of Personal Information**
  - The term “personal information” means, when not encrypted, an individual’s first name or first initial and last name in combination with any one or more of the following data elements:
    - Social Security number;
    - Driver’s license number or Minnesota identification card number; or
    - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

#### 4. Notification to Covered Entity

CyncHealth will notify Covered Entity’s designated privacy official, without unreasonable delay but in no event more than three (3) business days after discovery by Business Associate, any Use or Disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware, including any Breach of Unsecured Protected Health Information as required at 45 CFR 164.410 and as defined in Minnesota Statutes section 325E.61, and any Security Incident of which it becomes aware, together with any remedial or mitigating action taken or proposed to be taken with respect thereto.

#### C. Retention

The Privacy/Security Official shall maintain a log of all risk assessments and breach notifications made by the *CyncHealth* pursuant to this policy. The log should maintain documentation that all required notifications were made, or alternatively, of the risk assessment analysis that an impermissible Use or Disclosure did not constitute a Breach in cases where it was determined that a Breach did not occur. All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate all appropriate steps were completed. All supporting documentation associated with the potential Breach shall be maintained for a minimum of six (6) years.

#### D. Response Team



Should you identify a medium-impact or high-impact security incident as defined in the CyncHealth Incident Management Policy, open the *CyncHealth Cybersecurity Incident Response Plan* and follow the procedures as required.

**E. Miscellaneous**

1. The Privacy/Security Official shall maintain files of Incident Response investigations and meetings;
2. The policies and procedures relating to training, complaints, sanctions, refraining from intimidating or retaliatory acts, waiver of rights, policies and procedures and documentation (as required under 45 C.F.R. § 164.530(b), (d), (e), (g), (h), (i) and (j)) apply to the provisions outlined in these Breach Notification Procedures;
3. Capitalized terms not otherwise defined herein shall have the meanings assigned to them in the HIPAA regulations.

**DISCLOSING INFORMATION TO BUSINESS ASSOCIATE SUBCONTRACTOR**

<b>Document Group Title:</b> Minnesota Privacy Policies	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b>	<b>Approval Committee:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and contractors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
<b>Title</b>	<b>Title</b>	

**A. Policy Purpose:**

This policy establishes guidelines for the disclosure of patient health information to, and use by, a business associate subcontractor.

**B. Policy Implementation**

**1. General Rule**

A business associate is a person or entity that performs certain functions, activities, or services for or on behalf of CyncHealth that involves the use or disclosure of PHI.

If CyncHealth enters into a subcontractor Business Associate Agreement and obtains satisfactory assurance that the business associate will appropriately safeguard PHI, CyncHealth may disclose PHI to the business associate and allow that business associate to create, receive, maintain, or transmit PHI on CyncHealth’s behalf.

**2. Business Associate Agreements**

CyncHealth shall use a written agreement with its subcontractor business associates to ensure and document that its business associates will appropriately safeguard PHI received from CyncHealth.

If CyncHealth becomes aware of a pattern of activity or practice of the subcontractor that constitutes a material breach or violation of the subcontractor’s obligation under the contract or other arrangement, the business associate shall take reasonable steps to cure the breach or end the violation, as applicable. If the steps taken to cure the breach or end the violation are unsuccessful, the business associate shall terminate the contract, if feasible.

**4. Requirements for Business Associate Agreements**

A business associate agreement between CyncHealth and a business associate must:

- a. Establish the permitted and required uses and disclosures of PHI by the business associate. The agreement may not authorize the business associate to use or further





disclose the PHI in a manner that would violate the HIPAA Regulations or these policies if the use or disclosure was done by CyncHealth; However:

- i. The agreement may permit the business associate to use and disclose PHI for the proper management and administration of the business associate; and
  - ii. The agreement may permit the business associate to provide data aggregation services relating to the health care operations of CyncHealth.
- b. Provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
  - c. Provide that the business associate will use appropriate safeguards and comply, where applicable, with the HIPAA Regulations provisions pertaining to electronic protected health information, to prevent use or disclosure of ePHI other than as provided for by its contract;
  - d. Provide that the business associate will report to CyncHealth any use or disclosure of the PHI not provided for by its contract, whenever it becomes aware of such unauthorized use or disclosure, including breaches of unsecured PHI;
  - e. Provide that the business associate will ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate shall agree to the same restrictions and conditions that apply to the business associate with respect to the PHI;
  - f. Provide individuals access to PHI in accordance with these policies and the HIPAA Regulations;
  - g. Provide individuals the right to amend PHI in accordance with these policies and the HIPAA Regulations;
  - h. Provide individuals the right to an accounting of disclosures of PHI in accordance with these policies and the HIPAA Regulations;
  - i. Provide that to the extent the business associate is to carry out CyncHealth's obligations under the HIPAA Regulations, the business associate will comply with the requirements that apply to CyncHealth;
  - j. Require the business associate to make its internal practices, books, and records relating to the use and disclosure of PHI received from CyncHealth (or created or received by the business associate on behalf of CyncHealth) available to the Secretary of Health and Human Services for purposes of determining CyncHealth's compliance with the HIPAA Regulations;
  - k. Requires the business associate to report to CyncHealth any security incident of which it becomes aware, including breaches of unsecured PHI;

- l. At termination of the agreement, if feasible, return or destroy all PHI received from CyncHealth (or created or received by the business associate on behalf of CyncHealth) that the business associate maintains in any form (including copies of such information). If the return or destruction of the PHI is not feasible, the business associate shall extend the protections of the contract to the information and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the information infeasible; and
  - m. Authorize termination of the contract by CyncHealth, if CyncHealth determines that the business associate has violated a material term of the contract.
5. **Use and Disclosure of PHI by a Business Associate for the Business Associate's Own Management and Administration**

The business associate agreement between CyncHealth and a subcontractor business associate may permit the business associate to **use** (not disclose) the PHI received by the business associate, if necessary:

- a. For the proper management and administration of the business associate; or
- b. To carry out the legal responsibilities of the business associate.

The business associate agreement between CyncHealth and a business associate may permit the business associate to **disclose** the PHI received by the business associate for: (A) the proper management and administration of the business associate; or (B) carrying out the legal responsibilities of the business associate, if:

- a. The disclosure is required by law; or
- b. The business associate obtains reasonable assurances from the person to whom the PHI is disclosed that:
  - i. It will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and
  - ii. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

6. **Business Associate Contracts with Subcontractors**

The requirements of this policy apply to contracts or other arrangements between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contractors or other arrangements between CyncHealth and business associate.

When entering into arrangements with subcontractors, business associates should use the Template Subcontractor Business Associate Agreement, see Attachment A.

**7. Documentation Regarding a Business Associate Contract**

CyncHealth shall document and retain a business associate contract or memorandum of understanding, in written or electronic format for at least six (6) years from the date when the business associate contract or memorandum of understanding was last in effect.

**II. Procedure:**

- A. CyncHealth and its employees will determine whether an entity/vendor is a business associate in accordance with this policy.
- B. If an entity/vendor is a business associate of CyncHealth, Director or designee must contact the Privacy Officer to set up the needed written agreements.
- C. CyncHealth will only disclose PHI to a business associate in accordance with this policy and the written agreements.

**Attachment A**  
**Nebraska Health Information Initiative, Inc., DBA CyncHealth**  
**BUSINESS ASSOCIATE**  
**SUBCONTRACTOR AGREEMENT**

**THIS SUBCONTRACTOR AGREEMENT** (“Agreement”) is between Nebraska Health Information Initiative, Inc., DBA CyncHealth (“Business Associate”) and [name of vendor] (“Subcontractor”). This Agreement is effective as of the Effective Date set forth below.

1. **Definitions.** Terms used but not otherwise defined in this Agreement shall have the meaning ascribed in section 160.103, 164.501, or elsewhere, in the Regulations.
  - a. **“ePHI”** means PHI that is maintained or transmitted in electronic media.
  - b. **“Breach”** means, with respect to PHI, the impermissible acquisition, access, use or disclosure of Unsecured PHI which compromises the security or privacy of the PHI.
  - c. **“Subcontractor Functions”** means all functions performed by Subcontractor under one or more Service Agreements on behalf of Business Associate which involve the creation of, access to, use or disclosure of PHI by Subcontractor or its agents or subcontractors.
  - d. **“HIPAA”** means the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d to 1320d-7, and future amendment thereto and the Regulations issued thereunder.
  - e. **“PHI”** means protected health information as defined in the Regulations, which is created, obtained or used by Subcontractor in the performance of one or more Subcontractor Functions for Business Associate.
  - f. **“Regulations”** means the final Regulations implementing the privacy and security provisions of HIPAA as amended from time to time. The Regulations are presently codified at 45 C.F.R. Parts 160, 162 and 164.
  - g. **“Services Agreement(s)”** or **“Agreement”** means all agreements, whether written or oral, and whether now in effect or hereafter entered into, between Business Associate and Subcontractor for the performance of Subcontractor Functions by Subcontractor. Existing Services Agreement(s) are listed on attached Exhibit A.
  - h. **“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.
  - i. **“Unsecured PHI”** means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the methods outlined by the Department of Health and Human Services in 74 Fed. Reg. 19006 (2009) (to be codified at 45 C.F.R. §160 and §164).
2. **Purpose.** CyncHealth is a Business Associate under HIPAA to various covered entities (“Participants”) participating in the electronic exchange of information through the record locator service and other data exchange services provided by CyncHealth (“System”). Business Associate requires certain services of Subcontractor as detailed in the Services Agreement (“Subcontractor Functions”), which involves access to PHI of multiple Participants. HIPAA requires Business Associate to obtain satisfactory written contractual assurances from its subcontractors before furnishing them with PHI or permitting them to obtain or create PHI to perform functions on its behalf. This Agreement is entered into to provide Business Associate with the contractual assurances required under HIPAA.
3. **Permitted Uses and Disclosures of PHI.** Subcontractor shall only use and disclose PHI for the following purposes:

- a. To perform Subcontractor Functions.
- b. As needed for the proper management and administration of Subcontractor and to carry out the legal responsibilities of Subcontractor.

4. **Special Conditions on Disclosure for Subcontractor's Purposes.** Before Subcontractor may *disclose* PHI to another party for a reason described in subparagraph 3b, one of the following two conditions must be met; either –

- a. the disclosure must be *required by law*; or
- b. Subcontractor must obtain *reasonable assurances* from the person to whom the PHI is disclosed that such person will safeguard the PHI and further use and disclose it only as required by law or for the purpose for which Subcontractor disclosed it to such person; and such person must agree in writing to notify Subcontractor of any instances of which it is aware in which the confidentiality of the PHI has been breached.

5. **Assurances of Subcontractor.** As an express condition of performing Subcontractor Functions, Subcontractor agrees to:

- a. Comply with the requirements of Title XII, Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act, codified at 42 U.S.C. §§ 17921-17954, which are applicable to Subcontractor, and comply with all regulations issued by the Department of Health and Human Services (HHS) to implement HITECH, as of the date by which Subcontractor is required to comply with HITECH and the related regulations. Such requirements are hereby incorporated by reference into this Subcontractor Agreement.
- b. Use and disclose PHI only as permitted or required by this Agreement, or as otherwise required by law. Subcontractor shall not use or disclose information in a manner that would violate any applicable law if done by Business Associate.
- c. Use appropriate safeguards to prevent use or disclosure of PHI other than as provided for in this Agreement.
- d. Report to Business Associate's designated privacy official, without unreasonable delay but in no event more than five (5) business days of discovery by Subcontractor, any acquisition, access, use or disclosure of PHI not provided for in this Agreement or not permitted under the Regulations, including any impermissible access, acquisition, use or disclosure that is a Breach of Unsecured PHI, together with any remedial or mitigating action taken or proposed to be taken with respect thereto. Subcontractor shall conduct a risk assessment with respect to any impermissible access, acquisition, use or disclosure to determine if there is a significant risk of financial, reputational or other harm to the individual whose PHI was impermissibly acquired, accessed, used or disclosed. Subcontractor shall notify Business Associate of any such impermissible access, acquisition, use or disclosure, including the following information in such notice:
  - i. A brief description of how the impermissible access, acquisition, use or disclosure occurred and how and when it was discovered.
  - ii. A description of whether Unsecured PHI was involved in the impermissible access, acquisition, use or disclosure, and the results of Subcontractor's risk assessment.
  - iii. The steps Subcontractor is taking to further investigate the impermissible access, acquisition, use or disclosure, to mitigate losses, and to protect against further impermissible access, acquisition, use or disclosure.

Subcontractor shall cooperate with Business Associate in mitigating any harmful effects of any such impermissible access, acquisition, use or disclosure, and in making any required notification to individuals in the case of a Breach as determined by Business Associate. Subcontractor shall pay for the costs of such mitigation and notification if the Breach was due to a violation of this Agreement by Subcontractor, or the negligent or intentional actions of Subcontractor.

- e. Provide individuals with access to and copies of PHI maintained by Subcontractor in designated record sets, and limit fees for access and copying, all in accordance with Business Associate's obligations to individuals under 45 C.F.R. § 164.524.

f. Notify Business Associate within three (3) business days of any request by individuals to amend PHI maintained by Subcontractor in designated record sets, direct the requesting individual to Business Associate for handling of such request, cooperate with Business Associate in the handling of such request, and incorporate any amendment accepted by Business Associate in accordance with §164.526 of the Regulations. Subcontractor is not authorized to independently agree to any amendment of PHI.

g. Maintain a record of those disclosures of PHI by Subcontractor or its agents or subcontractors which are subject to the individual's right to an accounting under § 164.528 of the Regulations and report such disclosures to Business Associate within five (5) business days of request by Business Associate in a form permitting Business Associate to respond to an individual's request for an accounting.

h. Make its internal practices, books and records relating to the use and/or disclosure of PHI available to the Secretary of HHS or his or her designees for purposes of determining Business Associate's compliance with the Regulations.

i. Return to Business Associate or destroy (and not retain a copy) all PHI in its possession, upon the termination of the Services Agreement or as soon as such PHI is no longer needed by Subcontractor to perform its responsibilities hereunder, whichever comes first, and require its agents and subcontractors to do likewise. To the extent that return or destruction is not feasible, the protections of this Agreement shall remain in effect for so long as Subcontractor or its agents or subcontractors have possession of or access to such PHI, and Subcontractor agrees to limit further uses and disclosures of the PHI to those purposes which make return or destruction infeasible.

j. Ensure that all agents and subcontractors who will create, receive, use or disclose PHI to perform a Subcontractor Function under this Agreement agree in writing to adhere to the same restrictions and conditions on the use and/or disclosure of PHI that apply to Subcontractor.

k. Ensure that all other agents and contractors of Subcontractor who have access to PHI to perform other services (other than Subcontractor Functions) to Subcontractor agree in writing to take reasonable steps to safeguard the privacy of PHI.

l. Comply with any voluntary restriction on use or disclosure of PHI accepted by Business Associate under § 164.522(a) of the Regulations which is properly communicated to Subcontractor

m. Comply with any reasonable requests by individuals under § 164.522(b) of the Regulations to receive communications of PHI by alternative means or at alternate locations when communicated to Subcontractor by Business Associate or directly by the individual.

n. Limit the use and disclosure of PHI for purposes described in this Agreement to the minimum necessary to perform the required function. Subcontractor shall comply with any additional requirements for the determination of minimum necessary as are required from time to time by the Regulations, as amended.

6. **Security Assurances of Subcontractor.** If Subcontractor will create, receive, maintain or transmit ePHI on behalf of Business Associate, it further agrees to:

a. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of ePHI.

b. Ensure that any agent, including a subcontractor, to whom it provides ePHI, or with whom it contracts to create, receive, maintain or transmit ePHI, agrees to implement reasonable and appropriate safeguards to protect such ePHI.

c. Report to Business Associate any Security Incident of which Subcontractor becomes aware.

d. Comply with any other required provision of the Regulations, as amended by the HITECH Act.

7. **Responsibilities of Business Associate.** Business Associate agrees to:

- a. Notify Subcontractor promptly if Business Associate agrees to any voluntary restrictions on the use or disclosure of PHI which will affect Subcontractor's use or disclosure of PHI under the Services Agreement.
- b. Notify Subcontractor of any reasonable requests by individuals under §164.522(b) of the Regulations to receive communications of PHI by alternative means or at alternative locations, if such requests will affect Subcontractor's services.
- c. Provide Subcontractor with a copy of any amendment to PHI which is accepted by Business Associate under §164.526 of the Regulations which Business Associate believes will apply to PHI maintained by Subcontractor in designated record sets.

8. **Supervening Law.** Upon the enactment of any law or regulation affecting the use or disclosure of PHI, or the publication of any decision of a court of the United States or of this state relating to any such law, or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, Business Associate may, by written notice to Subcontractor, amend this Agreement in such manner as it determines necessary to comply with such law or regulation. If Subcontractor disagrees with any such amendment, it shall so notify Business Associate in writing within thirty (30) days of Business Associate's notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, either party may terminate the Services Agreement on not less than thirty (30) days' written notice to the other. If not so terminated, the amendment or amendments proposed by Business Associate shall become effective.

9. **Identity Theft Prevention Program.** Subcontractor acknowledges that Business Associate has adopted, or will adopt, an Identity Theft Prevention Program as required under 16 C.F.R. Part 681 ("Red Flags Rule") for certain covered accounts that may be accessed in accordance with the Service Agreement. Subcontractor acknowledges that it may be a Service Provider under Business Associate's Identity Theft Prevention Program. Accordingly, to the extent Subcontractor is a Service Provider as that term is defined in the Red Flags Rule, Subcontractor will conduct its activities in accordance with reasonable policies and procedures to detect, prevent and mitigate identity theft. Subcontractor shall report to Business Associate's compliance officer, within three (3) business days of a reasonably confirmed incidence of identity theft involving Business Associate's covered accounts, together with any remedial or mitigating action taken or proposed to be taken with respect thereto. Subcontractor shall cooperate with Business Associate in mitigating any harmful effects of any such activity.

10. **Term and Termination.**

a. **Term.** This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, including return or destruction of all PHI in Subcontractor's possession (or in the possession of Subcontractor's agents and subcontractors), unless sooner terminated as provided herein. It is expressly agreed that the terms and conditions of this Agreement designed to safeguard PHI shall survive expiration or other termination of the Services Agreement and shall continue in effect until Subcontractor has performed all obligations under this Agreement.

b. **Termination by Business Associate.** Business Associate may immediately terminate the Services Agreements, if Business Associate makes the determination that Subcontractor has breached a material term of this Agreement. Alternatively, Business Associate may choose to provide Subcontractor with written notice of the existence of an alleged material breach, and afford Subcontractor an opportunity to cure the alleged material breach upon mutually agreeable terms. Failure to take reasonable steps to cure the breach is grounds for the immediate termination of this Agreement.

c. **Termination by Subcontractor.** If Subcontractor determines that Business Associate has breached a material term of this Agreement, Subcontractor shall notify Business Associate and



provide Business Associate an opportunity to cure the alleged material breach upon mutually agreeable terms. Failure of Business Associate to take reasonable steps to cure the breach is grounds for the immediate termination of this Agreement.

d. **Return/Destruction infeasible.** In the event that Subcontractor determines that returning or destroying the PHI is infeasible, Subcontractor shall provide to Business Associate notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Subcontractor shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Subcontractor maintains such PHI.

11. **Miscellaneous.**

a. **Business Associate.** For purposes of this Agreement, and as applicable to the Subcontractor Functions of Subcontractor under all Service Agreements covered by this Agreement, references to Business Associate shall include the named Business Associate and all other entities covered by a joint Notice of Privacy Practices with Business Associate, whether as part of an affiliated Business Associate or an organized health care arrangement.

b. **Survival.** The respective rights and obligations of Subcontractor and Business Associate hereunder shall survive termination of this Agreement according to the terms hereof and the obligations imposed on Business Associate under HIPAA.

c. **Interpretation; Amendment.** This Agreement shall be interpreted and applied in a manner consistent with Business Associate’s obligations under HIPAA. Except as provided in Section 8 of this Agreement, all amendments shall be in writing and signed by both parties, except that this Agreement shall attach to additional Services Agreements entered into between the parties in the future without the necessity of amending this Agreement each time. This Agreement is intended to cover the entire Subcontractor *relationship* between the parties, as amended, from time to time, through Services Agreements or other means.

d. **Waiver.** A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

e. **No Third-Party Beneficiaries.** Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies or obligations.

This Agreement is effective \_\_\_\_\_ 2021.

**IN WITNESS WHEREOF**, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

Business Associate: Nebraska Health Information Initiative, Inc., DBA CyncHealth

**Subcontractor:**

Signature: \_\_\_\_\_

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date Signed: \_\_\_\_\_

Date Signed: \_\_\_\_\_



**USING AND DISCLOSING OF HEALTH INFORMATION**

<b>Document Group Title:</b> Minnesota Privacy Policies	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b>	<b>Approval Committee:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and contractors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
<b>Title</b>	<b>Title</b>	

**I. Policy**

**A. Purpose**

This policy establishes guidelines to be followed by CyncHealth’s workforce when using or disclosing information for Health Care Operations.

**B. Policy Implementation—General Rule**

Compliance with all laws

All disclosures and uses of health information through CyncHealth must be consistent with all applicable federal and state laws and CyncHealth policies. Disclosures and uses may not be used for any unlawful or discriminatory purpose. If applicable law requires that certain documentation exist (such as an authorization or consent) or that other conditions be met prior to using or disclosing health information for a particular purpose. In all cases, the requesting CyncHealth Participant shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of the documentation and conditions at the request of the disclosing Participant.

**C. Disclosure of Minimum Necessary**

When CyncHealth and its workforce uses and discloses PHI for Health Care Operations purposes, or discloses, it must comply with the minimum necessary rule. This means that it can use or disclose only the information that is necessary.

**II. Uses and Disclosures**

**A. Health Care Operations**

CyncHealth may use Participant’s shared information to provide data aggregation services as well as other Health Care Operations’ services relating to Participant’s and other users in accordance with the Policies and Procedures in the following circumstances:

1. Each entity either has or had a relationship with the individual who is the subject of the PHI being requested and the PHI pertains to such relationship, and the disclosure is:
  - a. For conducting quality assessment and improvement activities, or other activities discussed in subsection (i) of the definition of “Health Care Operations” (*see* CyncHealth’s Definitions Policy);
  - b. For reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, and other activities discussed in subsection (ii) of the definition of “Health Care Operations” (*see* CyncHealth’s Definitions Policy); or
  - c. For the purpose of health care fraud and abuse detection or compliance.
2. A covered entity that participates in an organized health care arrangement (an “OHCA”) may disclose PHI to other participants in the OHCA for any Health Care Operations activities of the OHCA; or
3. Pursuant to patient authorization that meets HIPAA standards.

## **B. HIPAA Authorizations**

The general rule is that except as otherwise permitted under the HIPAA Regulations, CyncHealth may not use or disclose PHI without valid authorization from the individual to whom the PHI pertains. CyncHealth must use or disclose PHI only in accordance with the authorization.

### 1. Authorizations for Use or Disclosure of Psychotherapy Notes

CyncHealth must obtain HIPAA authorization for any use or disclosure of Psychotherapy Notes. However, authorization is not required for the following:

- a. Use by the originator of the Psychotherapy Notes for treatment;
- b. Use or disclosure by CyncHealth for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling;
- c. Use or disclosure by CyncHealth to defend itself in a legal action or other proceeding brought by the individual;
- d. Use or disclosure that is required by the Secretary to investigate or determine
  - i. CyncHealth’s compliance with the HIPAA Privacy Rule;
- e. Use or disclosure that is required by law;
- f. Use or disclosure for health oversight activities by the originator of the Psychotherapy Notes;
- g. Use or disclosure about decedents to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law; or

- h. Use or disclosure to avert a serious threat to health or safety pursuant to 45 C.F.R. § 164.512(j)(1)(i).

2. Content of Valid Authorization, *see also* HIPAA Authorization Checklist

All authorizations must be written in plain language and contain at least the following elements:

- a. A specific and clear description of the information to be used or disclosed;
- b. The name or other specific identification of the person(s) or group of persons authorized to make the requested use or disclosure;
- c. The name or other specific identification of the person(s) or group of persons to whom CyncHealth may make the requested use or disclosure;
- d. A description of each purpose of the requested use or disclosure. The statement, “at the request of the individual,” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose;
- e. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statements, “end of the research study,” “none” or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository;

**Note:** The expiration date in Minnesota shall be one year from the time of issuance, or for a different period specified in the consent, consistent with Minnesota Statutes § 144.293, subd. 4;

- f. Signature of the individual and date;
- g. If the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual must also be provided;
- h. A statement of the individual’s right to revoke the authorization in writing, and either:
  - 1. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
  - 2. A reference to the entity’s Notice of Privacy Practice if the Notice of Privacy Practice includes a statement regarding exceptions to the right to revoke and a description of how the individual may revoke the authorization.
- i. A statement of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

1. The entity may not condition treatment on whether the individual signs the authorization when it is prohibited to do so; or
  2. The consequences to the individual of a refusal to sign the authorization when the entity may condition treatment on failure to obtain such authorization.
- j. A statement that the potential for information disclosed pursuant to the authorization to be subject to disclosure by the recipient and no longer be confidential by the HIPAA Regulations.

### **C. Marketing**

CyncHealth may use and disclose PHI for marketing purposes only in accordance with the HIPAA Regulations, applicable state law, and this Policy.

#### **1. Authorization for use or disclosure of PHI for marketing**

CyncHealth must obtain a valid HIPAA authorization, as defined by the Regulations, from the patient or a personal representative prior to any use or disclosure of PHI for “marketing” as defined in section 3 of this policy. The authorization required by this section must be a signed document that meets the requirements of 45 C.F.R. § 164.508 and this Policy.

### **D. Psychotherapy Notes**

CyncHealth does not request or retain psychotherapy notes as defined under HIPAA.

HIPAA Authorization Checklist

<b>Required Elements</b>		
<b>The following elements/statements <u>must</u> appear in a HIPAA authorization form.</b>		
<b>164.508(c)(1): Core Elements:</b> An authorization must include the following:	<b>Notes</b>	<b>Check-off</b>
(1) <b>Description.</b> A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion		
(2) <b>Name of disclosing person/entity.</b> The name (or other specific identification) of the person (or class of persons) authorized to use or disclose information.		
(3) <b>Name of receiving person/entity.</b> The name (or other specific identification) of the person (or class of persons) authorized to receive or use information		
(4) <b>Purpose.</b> A description of the purpose for the use or disclosure. The statement “at the request of the individual” is sufficient if the individual initiates the authorization and does not provide additional information regarding the purpose.		
(5) <b>Expiration date/event.</b> The statement, “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of PHI for research.		
(6) <b>Date/Signature.</b> The date and signature of the individual providing the authorization. If signed by an authorized representative, it must also include a description of the representative’s authority to act on behalf of the individual.		
<b>164.508(c)(1): Required Statements.</b> The authorization must include a statement describing:	<b>Notes</b>	<b>Check-off</b>
(1) <b>The right to revoke.</b> Must state that the individual has a right to revoke the authorization in writing and either: (A) the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (B) if exceptions to the right to revoke are addressed in the Notice of Privacy Practices, a reference to such Notice.		
(2) <b>Ability/Inability to condition services on authorization.</b> Must state either: (A) the CE may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs an authorization; or (B) the consequences to the individual of a refusal to sign the authorization.		
(3) <b>Redisclosure.</b> The potential for information disclosed to be subject to a redisclosure by the recipient and no longer protected by the Privacy Rule.		
<b>Other requirements</b>	<b>Notes</b>	<b>Check-off</b>
(1) <b>Plain Language.</b> The authorization must be written in plain language.		
(2) <b>Copy.</b> CE must provide the individual with a copy of the signed authorization.		

(3) <b>Compound authorizations.</b> The authorization is not combined with any other document unless: (1) the authorization is for use and disclosure of PHI		
--	--	--

<b>Required Elements</b>		
<b>The following elements/statements <u>must</u> appear in a HIPAA authorization form.</b>		
<p>for a research study, and it is combined with another type of written permission for the same or another research study (provided such compound authorization clearly differentiates between any conditioned and unconditioned research components on the provision of such authorization); (2) the authorization is for a use or disclosure of psychotherapy notes and is combined with another authorization for a use or disclosure of psychotherapy notes; (3) the authorization is combined with another authorization (other than an authorization for a use or disclosure of psychotherapy notes), provided a CE has not conditioned the provision of treatment, payment, enrollment in health plan, or eligibility for benefits on the signing of one of the authorizations (unless such authorization is for number (1) above).</p>		
(4) <b>Marketing.</b> If the authorization is for marketing, and the marketing involves financial remuneration to the CE from the third party, the authorization must state that such remuneration is involved.		
(5) <b>Sale of PHI.</b> If the authorization is for sale of PHI, the authorization must state that the disclosure will result in remuneration to the CE.		



**DISCLOSURES FOR JUDICIAL AND ADMINISTRATIVE PROCEEDINGS**

<b>Document Group Title:</b> Minnesota Privacy Policies	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b>	<b>Approval Committee:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and contractors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
Title	Title	

**The HIPAA Privacy Rule allows, but does not require, Covered Entities to disclose PHI without the patient’s consent in response to certain judicial and administrative processes. See 45 C.F.R. § 164.512(e). However, the Minnesota Health Records Act allows disclosure of health records without the patient’s consent only pursuant to “specific authorization in law.” Minn. Stat. § 144.293, subd. 2(2).**

**I. Disclosures for Judicial and Administrative Proceedings Policy:**

**A. Purpose**

This policy establishes guidelines for CyncHealth to follow regarding the disclosure of PHI in response to a subpoena, court order, or other lawful process originating from a judicial or administrative proceeding.

**B. In General**

In accordance with the requirements and restrictions outlined in this policy, CyncHealth may use or disclose PHI, without the written authorization of the individual or giving the individual the opportunity to agree or object, in response to an order of a court or administrative tribunal or some other mandate in applicable state or federal law, provided that CyncHealth discloses only the PHI expressly authorized by such order or mandate.

Alternatively, CyncHealth may disclose PHI in the context of judicial and administrative proceedings if this occurs pursuant to the written authorization of the patient. For information regarding the content of the authorization and other information about authorization forms, refer to Using and Disclosing of Health Information Policy.

**C. Minimum Necessary**

CyncHealth must limit its use and disclosure of PHI pursuant to this policy to the minimum necessary to accomplish the intended purpose of the use or disclosure. For information regarding the requirements of the minimum necessary rule, refer to policy Minimum Necessary Requests for, or Uses or Disclosures of, PHI.

**D. Minnesota Law**

CyncHealth may disclose PHI in the context of judicial and administrative proceedings pursuant to a request accompanied by a court order. Examples of court orders include: (a) Minnesota state court order; (b) Minnesota federal court order; (c) order signed by a Minnesota judge or administrative law judge; (d) subpoena accompanied by a Minnesota court order, etc.

CyncHealth may also disclose PHI in this context pursuant to another “specific authorization in law.” For example, Minnesota Statutes section 256B.27 provides that the Minnesota Commissioner of Human Services shall be allowed access to all personal medical records of medical assistance recipients for the purposes of investigating vendors of medical care or whether the medical care was medically necessary.

## **E. Other Disclosures Permitted by HIPAA**

### **1. Satisfactory Assurance**

Although the Minnesota Health Records Act may only permit disclosure of health records based on “specific authorization in law”—which is generally interpreted as requiring an order of a court or an administrative tribunal or some other mandate of federal or state law—HIPAA does not prohibit CyncHealth’s use or disclosure of PHI, without the written authorization of the individual or giving the individual the opportunity to agree or object, in the course of any judicial or administrative proceeding as follows:

- a. In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if CyncHealth receives “satisfactory assurance” from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request. Such “satisfactory assurance” shall require a written statement and accompanying documentation demonstrating that:
  - i. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual’s location is unknown, to mail a notice to the individual’s last known address);
  - ii. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
  - iii. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and: (A) No objections were filed; or (B) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.
- b. In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if CyncHealth receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a “qualified protective order” that meets the requirements of this policy. Such “satisfactory assurance”



shall require a written statement and accompanying documentation demonstrating that:

- i. The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
- ii. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

## **2. A Qualified Protective Order**

For the purposes of this policy a “qualified protective order” with respect to PHI means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- a. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
- b. Requires the return or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

## **3. Disclosure without Satisfactory Assurance**

HIPAA permits CyncHealth to disclose PHI in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, without receiving satisfactory assurance, if:

- a. CyncHealth makes reasonable efforts to provide notice to the individual, including sufficient information about the litigation or proceeding in which the PHI is requested, to permit the individual to raise an objection to the court or administrative tribunal; or
- b. CyncHealth makes reasonable efforts to provide notice to the individual, including sufficient information about the litigation or proceeding in which the PHI is requested, to permit the individual to seek a qualified protective order.

## **4. Documenting Disclosures of PHI under this Policy**

CyncHealth will document any disclosures under this policy and will retain the documentation associated with the disclosure for at least six (6) years from the date of the disclosure.

**MINIMUM NECESSARY FOR REQUESTS FOR, OR USES OR DISCLOSURES OF, PHI**

<b>Document Group Title:</b> Minnesota Privacy Policies	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b>	<b>Approval Committee:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and contractors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
<b>Title</b>	<b>Title</b>	

**I. Policy:**

**A. Purpose**

The purpose of this policy is to limit the use and disclosure of PHI to only that which is needed for the purpose of the disclosure, in situations where the minimum necessary principle applies.

**B. Policy Implementation – General Rule**

When using or disclosing PHI or when requesting PHI from another covered entity or business associate, CyncHealth or CyncHealth’s business associate shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

For all uses, disclosures, and requests where the minimum necessary rule applies, CyncHealth may not use, disclose, or request the entire medical record, unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

**1. Situations where the minimum necessary rule does not apply**

CyncHealth and its workforce are not required to comply with the minimum necessary rule in the following situations:

- a. Disclosures to a health care provider for treatment or requests for treatment;
- b. Uses or disclosures to the individual that is the subject of the information as:
  - i. Permitted under 45 C.F.R. 164.502(a)(1)(i);
  - ii. Required upon request for access; or
  - iii. Required under the individual’s right to an accounting of disclosures.
- c. Uses or disclosures pursuant to an authorization;

- d. Disclosures made to the Secretary of the Department of Health and Human Services;
- e. Uses and disclosures that are required by law; and
- f. Uses and disclosures required for compliance with the requirements of the HIPAA Regulations.

## 2. **Minimum Necessary Uses of PHI**

CyncHealth shall identify the job positions and/or persons in its workforce who need access to PHI to carry out their duties, along with the categories of PHI to which access is needed. For each position and/or person, CyncHealth shall make reasonable efforts to limit access to only the categories of PHI to which access is needed.

## 3. **Routine and Recurring Disclosures or Requests**

For any type of disclosure or request made on a routine and recurring basis, CyncHealth shall limit the PHI to the amount reasonably necessary to achieve the purpose of the disclosure or request. CyncHealth has a procedure that limits the PHI disclosed to the amount that is reasonably necessary to accomplish the purpose of the disclosure or request.

## 4. **Other Disclosures or Requests**

For all other disclosures or requests, CyncHealth must:

- a. Develop criteria designed to limit the request for or disclosure of PHI to the information reasonably necessary to accomplish the purpose for which the request or disclosure is made.
- b. Review requests for disclosure on an individual basis in accordance with such criteria.

## 5. **Disclosures where CyncHealth may rely on a requested disclosure as the minimum necessary**

In certain circumstances, CyncHealth may rely on the judgment of the person requesting the disclosure as to the minimum amount of information that is needed. In other words, CyncHealth does not need to independently confirm that it is providing only the minimum amount of information necessary to accomplish the intended purpose. This reliance is permitted when the request is made by:

- a. A public official or agency who states that the information requested is the minimum necessary for the stated purpose and the disclosure is for a purpose permitted under 45 CFR 164.512;
- b. Another covered entity;

- c. A professional who is a member of CyncHealth's workforce or a business associate of CyncHealth when the purpose of the disclosure is to provide professional services to CyncHealth, if the professional represents that the information requested is the minimum necessary; or
- d. A researcher with appropriate documentation or representations that comply with the HIPAA Regulations' requirements on uses and disclosures for research.



**CONSENT TO DISCLOSE HEALTH INFORMATION UNDER MINNESOTA LAW**

<b>Document Group Title:</b> Minnesota Privacy Policies	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b>	<b>Approval Committee:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and contractors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
<b>Title</b>	<b>Title</b>	

**I. Policy:**

**A. Purpose**

This policy establishes consent requirements for the disclosure of health information as required by the Minnesota Health Records Act.

**B. Background**

CyncHealth and its workforce and Participants are subject to many consent requirements under both state and federal law, which often creates confusion. For example, HIPAA and Minnesota law have different patient consent requirements and use different terminology. The general rule under HIPAA is that PHI may not be *used or disclosed* by CyncHealth unless the use or disclosure is specifically permitted by HIPAA or authorized by the patient. “Patient Authorization” under HIPAA refers to a very specific type of patient consent. However, Minnesota Law only addresses the *disclosure* of information and generally requires patient consent prior to such disclosure (as opposed to patient authorization required by HIPAA).

**C. Policy Implementation – General Rule (Patient Consent Required)**

Except as described in this policy or unless a disclosure is specifically authorized by law, CyncHealth shall not disclose an individual’s health information without a signed and dated consent authorizing the disclosure from the individual or the individual’s legally authorized representative.

**D. Representation From Provider Participant**

CyncHealth may disclose information when there is a representation from a provider that the provider holds a signed and dated consent from the patient authorizing the release, provided CyncHealth documents:

- The provider requesting the health records;
- The identity of the patient;
- The health records requested; and



- The date the health records were requested.

#### **E. Specific Authorization in Law**

CyncHealth may disclose health information without patient consent when it is required by law to do so. For example, birth and death records must be reported to the Department of Health. In addition, CyncHealth is required to disclose instances of tuberculosis. CyncHealth must document the release in the patient's health record.

#### **F. Permitted Disclosures without a Consent**

CyncHealth may disclose health information without patient consent:

1. For a Medical Emergency when CyncHealth is unable to obtain the individual's consent due to the individual's condition or the nature of the Medical Emergency;
2. To other health care providers within Related Health Care Entities when necessary for the current treatment of the individual;
3. To a health care facility licensed by Minnesota Statutes chapter 144, Minnesota Statutes chapter 144A, or to the same types of health care facilities licensed by chapter 144 and chapter 144A that are licensed in another state when a patient:
  - a. Is returning to the health care facility and unable to provide consent; or
  - b. Who resides in the health care facility, has services provided by an outside resource under 42 CFR section 483.75(h), and is unable to provide consent; or
4. When the disclosure is specifically authorized by law; and
5. When the disclosure is to the commissioner of health or the Health Data Institute under chapter 62J, provided that the commissioner encrypts the patient identifier upon receipt of the data.
6. When CyncHealth is releasing a deceased patient's health care records to another provider for the purposes of diagnosing or treating the deceased patient's surviving adult child.

#### **G. Patient Request for Release to Provider**

Participant shall be solely responsible for affording individuals their rights with respect to Participant's Shared Information, such as the rights of access and amendment, or requests for special restrictions on the use or disclosure of health information. CyncHealth shall not accept or process any requests from individuals for the exercise of such rights, but shall promptly forward any such requests to Participant. Participant shall not undertake to afford an individual any rights with respect to any information in the System other than Participant's Shared Information.



## **H. Provider Participant Consent Requirements**

Each CyncHealth Participant shall be provided with written information in plain language about the CyncHealth Health Information Exchange. The material shall describe the benefits of participation, risks of participation, how and where to obtain additional information, contact information, and a description as to how the Individual's health information will be used. In Minnesota individuals must be informed that they have the right to opt-out of participation in the Record Locator Service so that their health care records are not found or located as a mechanism to preserve an individual's right to privacy. Individuals have a right to change a prior election and must be provided information on how to exercise those options, at no cost to the Individual. If an Individual later changes a prior election, the Participant receiving the new election shall maintain that documentation and shall notify CyncHealth of the change.

In addition, each Participant shall revise its Notice of Privacy Practices to describe the uses and disclosures of protected health information contemplated through the Participant's participation in CyncHealth, if such a use and disclosure is not already addressed in the Notice. The Notice must meet the content requirements under the HIPAA Privacy Rule and comply with applicable laws and regulations. Participants shall individually determine whether their current Notice requires amendment to reflect their contemplated uses and disclosure of protected health information through. Participants may not commit CyncHealth to any additional obligations or liabilities through the Notice.

## **I. Documentation of Release**

In addition to the documentation requirements specifically identified in this policy and other CyncHealth policies, CyncHealth must:

1. When releasing health records without patient consent as authorized by law, document the release in the patient's health record; and
2. When releasing mental health records to law enforcement according to Minn. Stat. § 144.294, subdivision 2, document the release in the patient's health record along with:
  - a. The date and circumstances for the disclosure;
  - b. The person or agency to whom the release was made; and
  - c. The records that were released.

## **II. Procedure:**

Except for disclosures permitted without consent, CyncHealth Participants shall obtain prior written consent for the disclosure of health information prior to disclosing such information.

**EXCHANGING INFORMATION WITH OUT-OF-STATE PROVIDERS**

	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b>	<b>Approval Committee:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and contractors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
<b>Title</b>	<b>Title</b>	

**I. Policy:**

**A. Purpose**

This policy establishes guidelines to be followed by CyncHealth’s workforce when exchanging patient health information with out-of-state providers.

**B. Policy Implementation—General Rule**

Both CyncHealth and an out-of-state provider are subject to federal laws, such as HIPAA. However, CyncHealth and an out-of-state provider are subject to different state laws.

CyncHealth and Participants operating in Minnesota must comply with Minnesota law when disclosing patient information to an out-of-state provider. Conversely, the out-of-state provider must comply with its state law when disclosing patient information to CyncHealth.

**C. Releasing Information to an Out-of-State Provider**

CyncHealth Minnesota Participants must comply with Minnesota law when releasing information to an out of-state provider. CyncHealth staff should refer to policy Consent to Use and Disclose Health Information under Minnesota Law for more information about disclosures under Minnesota law.

**D. Obtaining Information from an Out-of-State Provider**

An out-of-state provider is required to comply with its state law when it releases information to CyncHealth. This may cause operational barriers for CyncHealth, as the out-of-state provider may be subject to rules and requirements that CyncHealth is not familiar with.

It is ultimately the out-of-state provider’s responsibility to understand and comply with its state law when disclosing information to CyncHealth. However, to the extent it is feasible, CyncHealth staff should facilitate the exchange when it is in the best interests of the patient.



**AUTHORIZED PURPOSES FOR REDISCLOSURE OF PART 2 DATA**

<b>Policy:</b> Redisclosure of Part 2 Data – Authorized Purposes	<b>Accountability:</b> Systems Support Manager / CyncHealth Staff / Vendors:	
<b>Effective Date:</b>	<b>Review Date:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and vendors working on behalf of CyncHealth.		
<b>Approval:</b>	<b>Approval:</b>	
<b>Title:</b>	<b>Title:</b>	

**STATEMENT**

In accordance with the standards set forth under the Health Insurance Portability and Accountability Act (“HIPAA”) as well as federal and state statutory and regulatory requirements (hereafter referred to as “Regulatory Requirements”), CyncHealth is committed to ensuring the confidentiality, integrity, and availability of protected health information and electronic protected health information (PHI/ePHI), as well as any sensitive and confidential data it creates, receives, maintains, and/or transmits. For the purposes of this policy, PHI, ePHI and sensitive and confidential data shall be referred to herein as “Covered Information.”

Federal regulations at 42 CFR Part 2 (“Part 2 regulations”) require additional privacy protections for the maintenance, redisclosure, and destruction of data and records that are subject to Part 2 regulations.

**DEFINITIONS**

- **Electronic Health Information:** Electronic protected health information (ePHI) as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but shall not include (1) psychotherapy notes as defined in 45 CFR 164.501; or (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- **Health Information:** Protected health information (PHI) as defined in 45 C.F.R. §160.103 that is created, transmitted, or received by a Participant.
- **Part 2 Data:** Any data that is contained in a Part 2 Record, is subject to the protections of Part 2 regulations, and/or would identify a patient as having or having had a substance use disorder (SUD) either directly, by reference to publicly available information, or through verification of such identification by another person.
- **Part 2 Program:** A facility, department or unit within a facility, or an individual provider who holds itself out for SUD diagnosis, referral, and/or treatment services AND is federally assisted. (*Note:* the U.S. Armed Forces and the Department of Veterans Affairs are exceptions and are not Part 2 Programs.)

- **Part 2 Record:** Any information created by, received by, or acquired by a Part 2 Program relating to a patient (e.g., diagnosis, treatment and referral for treatment information, billing information, emails, voicemails, and texts). These

The purpose of this policy is to ensure that any and all redisclosures of Part 2 Data by CyncHealth and any entities acting on CyncHealth's behalf (e.g., technology vendors) are for authorized and allowable purposes only.

#### SCOPE AND APPLICABILITY

This policy covers all Part 2 Data that is redisclosed through a server or system owned, operated, rented, leased, or otherwise managed by CyncHealth or disclosed through CyncHealth or any of its affiliate entities, including but not limited to the Nebraska Healthcare Collaborative.

#### ROLES AND RESPONSIBILITIES

The Chief Data Officer (CDO) and Chief Legal Counsel will be responsible for the enforcement, interpretation, management, review, and education of this policy. Likewise, CyncHealth staff will be responsible for acknowledgement and adherence to this policy.

#### POLICY

##### **CyncHealth's Part 2 Consent for Redisclosure Form States Authorized Purpose: *Treatment***

In accordance with § 2.31(a)(5), CyncHealth's Part 2 Data Consent for Redisclosure form must include the purpose(s) for which CyncHealth may redisclose an individual's Part 2 Data.

The single purpose listed in this consent form is Treatment, which means that CyncHealth may only redisclose the individual's Part 2 Data for Treatment purposes (as such purposes is defined by HIPAA), as that is the only purpose the individual has consented to.

The Consent for Redisclosure form may be updated to include additional purposes only by approval from CyncHealth's Data Governance Committee. In the event of an update to the purposes listed in the consent form, this policy must also be reviewed and updated to align with any changes approved by the Data Governance Committee.

##### **Purposes For Which CyncHealth Will NOT Redisclose Part 2 Data: *Non-Treatment Purposes***

CyncHealth does not collect consent for the redisclosure of Part 2 Data for any reasons other than Treatment. Therefore, redisclosure of Part 2 Data for any purpose or use other than Treatment is unauthorized and likely to be out of compliance with Part 2 regulations.

Purposes and uses for which CyncHealth does NOT have required consent to redisclose Part 2 Data include, but are not limited to:

- Health Care Operations and/or Payment purposes, including by not limited to:
  - Billing, claims management, data processing
  - Quality assessments and improvement activities
  - Underwriting, enrollment, or other health insurance/benefits-related activities
  - Business planning, development, or administration
  - Customer service, patient safety activities, or review of health care services
  - Care coordination and/or case management

- Risk adjustment; determination of eligibility or coverage
- Disease Management
- Research data and/or data sets containing any of the identifiers listed in [§164.514\(b\)](#)

COMPLIANCE

Workforce members will be required to comply with all policies and procedures as a condition of employment or contract with CyncHealth. Workforce members who fail to abide by the requirements outlined in the CyncHealth policies and procedures will be subject to disciplinary action up to and including termination of employment or contract.

ANNUAL REVIEW

<b>Date:</b>	<b>Reviewed By:</b>	<b>Comments/Updates:</b>
<b>Date of implementations:</b>		<b>Date of updates:</b>

**Attachment C  
Consumer Opt-Out Procedure**

## Consumer Opt-Out Procedure

<b>Procedure:</b> Consumer Opt -Out	<b>Accountability:</b> CyncHealth Staff / Contractors / Workforce Members / Vendors	
<b>Effective Date:</b> May 1, 2020	<b>Review Date:</b>	<b>Referenced Policies:</b>
<b>Intended Audience:</b> All CyncHealth staff and vendors working on behalf of CyncHealth.		

### PROCEDURE

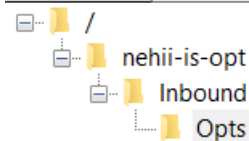
All Minnesota residents can opt out of CyncHealth.. The ONLY person that can opt a patient in and out is the patient themselves unless they are a minor, have a medical power of attorney or power of attorney.

1. Request is made directly by **consumer** by phone, webform or snail mail -
  - a. Phone – Requestor must validate 6 out of the 7 pieces of personal information from the list below: \* are required
    - i. First Name \*
    - ii. Last Name \*
    - iii. Middle initial \*
    - iv. Date of Birth \*
    - v. Address
    - vi. Phone number
    - vii. Facilities visited
  - b. Webform: via [Opt In/Out \(teamdynamix.com\)](http://Opt In/Out (teamdynamix.com))
    - i. Validate that the patient is in the system
    - ii. Call them at the number provided on the webform
    - iii. Follow the Phone validation process
      1. If no answer leave a message if possible “This is your name from CyncHealth calling to confirm a request we received via our web portal. Please call us back at 402-506-9900 option 1 to confirm this request.” (It is very important that when leaving a message that we do not leave any identifiable information from the request for HIPAA reasons.) Try 3 times and on the third time leaving a message let them know that their request will not be processed if we do not receive a call back.
      2. Move their request to the unprocessed request folder in box.
  - c. Snail Mail
    - i. Follow the same process as the webform.
    - ii. Support finds the record in the Clinical Viewer to note:
  - d. Assigning Authority (facility acronym)
  - e. MRN
  - f. MPIID if it is an Opt In

Identifier(s)	Name
i.  1000292864...	zztest, eight

- g. Set Consent Value Field to 0 for Opt out or 1 for Opt In.
- h. Set Status to Pending Provisioning.

- i. If you find duplicate records, follow the merge process
2. Export the Opt In/Out report from TDX and save it as a .CSV in Box\Departments\Information Systems\Opt Out Requests. Name the file OptInOutYYYYMMDD
3. Remove the First three columns from the report and Save it again. Only the following columns should remain on the report.
  - a. Assigning Authority(if opt out)
    - i. Cannot user NESIIS or XCADocuments
  - b. MRN (if opt out) from the assigning authority
  - c. First Name
  - d. Last Name
  - e. DOB
  - f. Address
  - g. City
  - h. State
  - i. Zip
  - j. Opt in consent value will be a 1 or Opt out consent value will be a 0
  - k. MPIID (if opt in)
4. [Login to Filezilla \(or any other SFTP client\) with the credentials that engineering has provided](#)
  - a. On the left side of the screen is your computer directory, the right is the SFTP location.



- b. Drill down of the right until you are in the OPTS folder:
  - c. Double click on the file that you just created (on the left) and would like to send to ISC to be processed.
    - i. Once the transfer is complete you will see it in the OPTS folder on the right. ISC should pick up the file within about 5 minutes. When this happens, the file will no longer be in the OPTS folder and you can sign out and close this application.
  - d. Go back to the spreadsheet and verify in the Clinical Viewer that all patients have been processed correctly
5. Close the associated tickets in Team Dynamix noting that it was processed and validated.
  6. Once all patients are Processed, the .csv can be moved to the "completed" subfolder.

**Attachment D  
Opt-Out Policy**

# Opt-Out Policy

<b>Policy:</b> CyncHealth Opt-Out Policy	<b>Accountability:</b> Systems Support Manager / CyncHealth Staff / Vendors:	
<b>Effective Date:</b> 12/9/2021	<b>Review Date:</b>	<b>Referenced Procedures:</b>
<b>Intended Audience:</b> All CyncHealth staff and vendors working on behalf of CyncHealth.		
<b>Approval:</b> CyncHealth Board of Directors	<b>Approval:</b>	
<b>Title:</b>	<b>Title:</b>	

## STATEMENT

In accordance with the standards set forth under the Health Insurance Portability and Accountability Act (“HIPAA”) as well as federal and state statutory and regulatory requirements (hereafter referred to as “Regulatory Requirements”), CyncHealth is committed to ensuring the confidentiality, integrity, and availability of protected health information and electronic protected health information (PHI/ePHI), as well as any sensitive and confidential data it creates, receives, maintains, and/or transmits. For the purposes of this policy, PHI, ePHI and sensitive and confidential data shall be referred to herein as “Covered Information.”

## DEFINITIONS

- **Electronic Protected Health Information (ePHI):** Information that is “individually identifiable health information” and is created, received, maintained, or transmitted in any electronic form or medium.
- **Protected Health Information (PHI):** Information that is “individually identifiable health information” and is created, received, maintained, or transmitted in any form or medium.
- **Opt-Out:** A request to restrict the sharing of a patient’s health information that is viewable through the clinical viewer within the platform.

## PURPOSE

The purpose of this policy is to document and regulate the CyncHealth policy and process for patient opt-out requests in accordance with Minnesota legislation, as well as compliance with CyncHealth policies that involve opt-outs. The objective is to provide clarity surrounding a patient’s right to opt-out from the CyncHealth Health Information Exchange. This policy seeks to establish parameters in compliance with Regulatory Requirements related to limited and proper disclosure of health data by ensuring CyncHealth staff are aware of the requirements and expectations surrounding opt-out requests made by patients.



## SCOPE AND APPLICABILITY

This policy covers CyncHealth patient opt-outs.

## ROLES AND RESPONSIBILITIES

The CyncHealth Chief Legal Counsel will be responsible for the enforcement, interpretation, management, review, and education of this policy. Likewise, CyncHealth staff will be responsible for acknowledgement and adherence to this policy.

## POLICY

### Opt-Outs

All individuals will have the opportunity to opt-out of participating in the health information exchange. A request to opt out will be treated as a request for restrictions on use and disclosure of Covered Information viewable within the health information exchange.

### Request Process

CyncHealth will provide notification on opt-out platforms on a public website.

An opt-out request will be initiated and accepted in digital and written notifications; a telephone request may be accepted if the identity verification process is met through a written form sent and returned to the address available in the demographic data. In addition, CyncHealth may upon request send a paper document to the individual for the purposes of opt-out. Once an opt-out is received and validated by the organization, the organization will process the opt-out within 30 calendar days.

### Participant Communication

Participants may access and download data sharing educational material on the health information exchange website. The education material will also contain a link to the health information exchange website where an explanation of the meaning and effect of participation or opting-out and a tool for opting-out or revoking a prior opt-out election will be available. CyncHealth will define the scope of an opt-out applied to the individual health information to include the advantages/disadvantages of the opt-in or opt-out.

CyncHealth participation agreements shall state that the Participant will not withhold coverage or care from an individual on the basis of that individual's choice not to have information viewable in the System. Participants will have collateral material available to individuals and designated to answer questions about data sharing via exchange networks to include CyncHealth.

CyncHealth will document procedures and train the support staff on the process for identity verification of the consumer.

The CyncHealth Compliance Committee will approve and review annually the communication to

consumers on the opt-out process that is posted to the public website.

## Opt-Out Impact

If an individual chooses to opt-out of participating in the health information exchange, the effect is applied as follows:

- i. an individual's clinical data will not be accessible by search or query by a participant user of the health information exchange application only; and
- ii. an individual's data will still flow into the HIE but will not be viewable.

An individual's decision to opt-out of participating in the health information organization:

- i. may be changed at any time by the individual by providing electronic or written notice to the support desk of the health information exchange;
- ii. does not prohibit use or disclosure of individually identifiable health information which is required by law; and
- iii. does not apply to all systems or applications operated by CyncHealth (i.e., public health applications such as PDMP or eMPI).

An Individual may opt-out of participation with an exception providing permission to access health information in the case of a medical emergency or if a disclosure is required by law. CyncHealth will facilitate this through a break the glass function and with the ability to audit these functions.

A participating health care provider will still be able to select the health information exchange as a way to receive that individual's lab results, radiology reports, and other data sent directly to any treating health care provider that the provider may have previously received by fax, mail, or other electronic communications. This information may be provided in a limited data set or via direct secure message or notifications required under the final interoperability rule [85 FR 25510].

## COMPLIANCE

CyncHealth staff will be required to comply with all information security policies and procedures as a condition of employment or contract with CyncHealth. CyncHealth staff who fail to abide by the requirements outlined in the CyncHealth Opt-Out Policy and Procedures will be subject to disciplinary action up to and including termination of employment or contract.

**Attachment E**  
**Certificate of Good Standing**



**Attachment F  
Hiring Policy**

## CyncHealth Advisors, Inc. Hiring Policy

### Objective

To hire qualified candidates who will support CyncHealth's mission. Recruitment should be timely, organized, and remain mindful of the candidate experience.

### Process

#### Position Requisitions

All newly created positions or increases to the headcount must be approved by the CEO prior to recruitment efforts beginning. The hiring manager can initiate the requisition process by submitting the completed requisition form to Human Resources. It will be reviewed by the CEO and CFO.

Open positions due to staff turnover do not require a requisition form to be completed.

#### Position Postings

Open positions will be posted on the CyncHealth's ApplicantStack job board and launched to Indeed, Google Jobs, and LinkedIn. The organization reserves the right to not publicly post an opening. Additional postings may be made at the discretion of Human Resources.

#### Internal Transfers

To be eligible for a posted job, employees must have performed satisfactorily for at least 90 calendar days in their current position or at the discretion of the CyncHealth CEO. Employees who have current written warning on file or are on probation or suspension are not eligible to apply for posted jobs without approval from the CEO.

Interested employees should contact Human Resources to learn more about the opportunity. They should also discuss their interest with their supervisor which can be done prior to speaking with Human Resources or following an initial conversation. Human Resources will seek feedback from the employee's current manager regarding performance and potential fit.

If the interested employee possesses the required skills, competencies, and qualifications, an interview will be scheduled with the hiring manager. If the employee is identified as a fit for the open position, the hiring manager will work with Human Resources and the employee's current supervisor on a transition plan. If the employee's qualifications do not align with the position, the employee will be notified and provided feedback on development opportunities that will better align them for future opportunities.

## Interview Training

All employees who will participate in the interview process must complete a formal training with Human Resources prior to their first interview. This training will cover CyncHealth expectations, legal considerations, and tips for a successful interview. Interviewers will need to sign off on this policy confirming their commitment to the expectations.

## Interview Process

All external candidates are required to submit a formal application through CyncHealth's applicant tracking system (ATS). This will ensure all candidate information is retained in a centralized location. Human Resources will screen all applications upon receipt and conduct an initial phone interview with candidates whose qualifications align with the position. If Human Resources believes the candidate may be a match for the position, interview notes and a resume will be forwarded on to the hiring manager.

If the hiring manager agrees that the candidate may be fit, an in-person interview will be scheduled. The hiring manager should ask questions that will determine the candidate's fit for the role. Depending on the position, candidates who are identified as a fit during the in-person interview will move on to a second in-person interview with additional stakeholders. Once all in-person interviews are complete, if the manager feels that the candidate has a high likelihood of success in the role, a reference check will be completed. If favorable references are obtained, an offer approval will go to the CFO and the department Chief.

## Staffing Agencies

All staffing agency contact should be directed through Human Resources to ensure contract compliance and centralized consideration of budget constraints. Contracts with staffing agencies must be reviewed by the legal department prior to signing. Staffing agency contacts who reach out to non-HR staff should be redirected to Human Resources.

## Pre-Employment Screening

Offers of employment are conditional on the successful outcome of a background check, drug screen, and reference check.

In instances where negative or incomplete information is obtained, the appropriate management and Human Resources will assess the potential risks and liabilities related to the job's requirements and determine whether the individual should be hired. If a decision not to hire or promote a candidate is made based on the results of a background check, there may be certain additional Fair Credit Reporting Act (FCRA) requirements that will be handled by Human Resources in conjunction with the employment screening service.

A reference check may be waived if the candidate is sufficiently known to the organization prior to seeking an employment opportunity.

### Offer

Candidates selected for a position will be provided an offer letter outlining the terms of the offer. Candidates who were not selected for the position will be notified through the ATS. Position postings will be removed from any applicable job boards and the position status will be changed to closed in the ATS. Staffing agencies recruiting for the position will be notified.

## Contract Positions

Contractors will be required to submit a resume for consideration but will not need to complete an application. Candidates for contract openings will have an interview with the position supervisor and any relevant stakeholders. If the position supervisor believes the candidate is a fit for the role, they will notify Human Resources who will complete all necessary paperwork with the staffing agency. New contracts or staffing documents must be reviewed by legal prior to signing. The staffing agency is responsible for the background check and drug screen.

## Acknowledgment

*I have read and understood the above policy. I agree to abide by the terms of the policy and seek guidance from Human Resources if I have any questions.*

Signature: \_\_\_\_\_ Date: \_\_\_\_\_



**Attachment F  
Accounting Policy**

# Accounting Policies

## Table of Contents

Background Information .....	3
Tax Status and Purpose .....	3
Service Area .....	4
Division of Responsibilities .....	5
Chart of Accounts.....	5
Accounting Principles.....	5
Revenue Recognition .....	5
Matching of Revenues and Expenses .....	5
Fixed Assets and Depreciation.....	6
Donated Materials and Services .....	6
Data Cutoff .....	6
Cash Disbursements.....	7
Capital Acquisitions .....	7
Supplies, Services, and Other Invoices .....	7
Invoice Payment.....	8
Payroll.....	8
Expense Reimbursements.....	8
Cash/Check Receipts .....	9
Bank Reconciliations.....	9
End of Month Accounting.....	10
End of Year Accounting.....	10
Cost Allocations.....	10
Investments.....	10
Debt.....	11
Reserves and Designated Funds .....	11
Internal Controls and Financial Audit .....	11
Compliance.....	12

Budgeting .....	13
Software Authorization and Backup .....	13
Record Retention .....	13
Maintenance of Accounting Policies Manual.....	13
Preparation of Tax Returns .....	14
Property and Equipment Inventory.....	14
Grants and Contracts .....	15
Revision Tracking .....	16

## Tax Status and Purpose

The following manual is a description of the policies for the accounting function of Nebraska Health Information Initiative, Inc. (NEHII, Inc) and its controlled organizations. NEHII, Inc. is a not-for-profit organization incorporated as an Internal Revenue Code (IRC) section 501(c)(3) organization. NEHII, Inc. is registered with the Secretary of State in Nebraska with a calendar year end. The articles of incorporation state that the purposes of NEHII, Inc. shall include:

1. Provide Nebraska with a system for the secure exchange and use of health information;
2. Be a leader in the secure exchange of health information enabling a healthier Nebraska;
3. Enable the sharing of timely and accurate patient healthcare information in a secure environment to improve patient care;
4. Provide a seamless, electronic patient-centric health information exchange allowing authorized access to health information;
5. Improve the health status of the residents of Nebraska;
6. Improve quality and safety in the delivery of healthcare throughout the state by facilitating the sharing of health information;
7. Support state and federal initiatives to improve healthcare quality and safety and to reduce cost through shared access to health information;
8. Establish the basis for development of state-wide and regional electronic health records in Nebraska as a means to improve quality, reduce errors, and control healthcare costs;
9. Support efforts to improve patient care, improve the quality of healthcare and reduce healthcare costs through data analytics;
10. Conduct and support healthcare education for students, graduate students, providers, and other healthcare workers in Nebraska; and
11. Monitor and recommend strategies to assist Nebraska providers to comply with state and federal technology standards and mandates in the healthcare field.

In accordance with IRC section 501(c)(3), NEHII, Inc. is organized and operates exclusively for the exempt purpose as described in Form 1023, the application for exemption. In compliance with the restrictions on organizations qualifying under IRC section 501(c)(3):

1. No part of the net earnings of the organization may inure to the benefit of any private shareholder or individual;
2. No substantial part of the activities of the organization may consist of the carrying on of propaganda or otherwise attempting to influence legislation;
3. The organization may not participate in, or intervene in, any political campaign on behalf of any candidate for public office.

NEHII, Inc is organized as a public charity under IRC section 509(a)(2) of the Internal Revenue Code as an organization that normally receives more than 1/3 of its support from contributions, membership fees, and gross receipts from activities related to its charitable, etc. functions, and no more than 1/3 of its support from gross investment income and unrelated business taxable income.

The following accounting policies are for NEHII, Inc. and its controlled organizations hereby known within this document as "NEHII". Controlled organizations include the following:

- Nebraska Healthcare Collaborative, Inc. – An IRC section 501(c)(3) organization organized to support NEHII Inc. by collaborating with the universities, the government and surrounding healthcare organizations to improve healthcare through research and development powered by healthcare data analytics.
- NEHII Foundation, Inc. – An IRC section 501(c)(3) organization organized to support NEHII Inc. by providing funding for healthcare-related, educational and scientific activities in support of the purposes of NEHII, Inc. for the improvement of, and access of, healthcare throughout Nebraska and surrounding areas.
- NEHII Shared Services Inc. – A wholly owned for-profit sub-subsiidiary of NEHII, Inc. to provide administrative services to all the organizations of NEHII, and consulting services to other healthcare industry entities, including, but not limited to other health information exchanges.

## Service Area

The primary service area is the State of Nebraska and western Iowa.

## Division of Responsibilities

See attached Addendum 1

## Chart of Accounts

NEHII has designated a chart of accounts specific to its operational needs and the needs of its financial statements. The chart of accounts is structured so that financial statements can be shown by natural classification (expense type) as well as by functional classification (program vs. fundraising vs administration).

The Director of Accounting is responsible for maintaining the chart of accounts and revising it as necessary. The chart of accounts is attached to this manual. See attached Addendum 2

## Accounting Principles

The accounting principles of NEHII will be consistent with all applicable laws. These include: Generally Accepted Accounting Principles (GAAP), Statements of Financial Accounting Standards Numbers 93, 116 and 117, SOP 94-2 on the applicability of the accounting rules to nonprofits, and SOP 98-3 on accounting for federal awards.

The Chief Financial Officer will not make entries into the general ledger.

Certain policies resulting from these accounting pronouncements and releases are discussed below.

## Revenue Recognition

Grants which are classified as exchange transactions with the grantor will be recognized as revenue when the grant money is earned. This will generally be determined by the costs reportable to the grantor. Each restricted grant will be tracked separately to allow for accurate and consistent recording of the investment income and expenses of each grant.

## Matching of Revenues and Expenses

In order to present accurate and consistent financial statements, the revenues and expenses attributable to each period will be reflected in that period to the degree possible. Generally, all entries required to accurately reflect the revenues and expenses of each period will be made in that period.

The organization records transactions on the accrual basis of accounting.

## Fixed Assets and Depreciation

The general capitalization policy is that all equipment and other fixed assets costing in excess of \$5,000 with a useful life greater than one year will be recorded as an asset. To determine if a repair or improvement will need to be capitalized, the following additional factor needs to be considered: does the expenditure extend the useful life of the asset repaired or improved? For example, painting would not be capitalized, but replacing a server or repairing the roof would be capitalized, if the dollar value was in excess of \$5,000.

All capital assets will be depreciated over their estimated useful lives. The straight- line basis will be used, with depreciation charged beginning in the month that the asset is placed in service. Some sample estimated lives are:

Computers and related equipment -	Three years
Office furniture -	Five years
Leasehold improvements -	15 years, limited to remaining lease term

Capital assets will not be purchased with government grants.

## Donated Materials and Services

Generally donated materials, assets and services will not be recorded in the accounting records.

In order to comply with the rules of SFAS 116, certain services would be recorded as revenues and expenses. Such services would be those professional services which we would otherwise have paid for which were provided by a person whose work would normally include providing those services.

Any donated assets which would meet the definition to be capitalized, outlined in the previous section, will be recorded as revenue and as a fixed asset.

## Data Cutoff

In order to meet the deadlines for producing reports discussed in the End of Month and End of Year sections, the gathering of information to use in making the month end entries must be cutoff by a certain date.

The monthly financial statements are due to the Board by the 25<sup>th</sup> day after month- end. For these reports a cutoff of 10 business days will be used. Any payables or other information not available by the 10<sup>th</sup> business day after a month end will be classified in the next period. The Director of Accounting may need to use estimates if final information is not available on a significant transaction.

The year-end financial statements are due to the Board eight weeks after year-end. For these reports a cutoff of 31 days will be used. Since the year end is the most

important period cutoff, the general ledger will continue to be held open for additional material transactions through the conclusion of the financial audit fieldwork.

## Cash Disbursements

The positions authorized to sign checks are: Chief Executive Officer, Chief Financial Officer and Board Treasurer. Only one signature will be required on checks. Anyone signing a check must review and confirm approval of the supporting invoice or other documentation. Approval can be via initials or signature on paper or through OneDesk or email. Individuals may not sign a check payable to themselves.

The Accountant II will maintain the accounts payable system. Prior to payment, the Director of Accounting will approve the coding for each invoice, authorize the checks and confirm the supporting documentation is appropriate.

The Accountant II prepares invoice payments using Bill.com or via paper check, if immediate payment is necessary.

The Human Resources Generalist will determine payroll amounts based on timesheets and authorized rates. The Human Resources Manager will complete a detailed review and then authorize payroll processing after approval by the Chief Financial Officer is received.

## Capital Acquisitions

Three bids are required for the purchase of budgeted capital assets in excess of \$100,000, if practical.

The Chief Executive Officer or designee selects a bidder. Board approval is required if the low bidder is not selected, if bidding was deemed impractical by the Chief Executive Officer, or if the amount is over \$500,000. Any capital assets not budgeted by the Board must be approved by the Board prior to soliciting bids.

Capital assets will not be acquired using government grant funding (either direct or pass-through) unless specifically required by the grant. If capital assets are acquired for this reason with grant funds, their use and disposition will comply with the requirements of 2 CFR 200.313.

## Supplies, Services, and Other Invoices

Chiefs, Directors, and the Office Manager can authorize purchases and payments in their areas provided there remains enough money in the budget.

Unbudgeted expenses require approval as defined in the Division of Responsibilities section above.



## Invoice Payment

Invoices are paid on their due date if the invoice specifies a date or sooner to take advantage of available prompt payment discounts. If no due date is specified invoices should be paid within 30 days of invoice date.

Invoices from subcontractors that are subject to pass through reimbursement via state or federal contracts are not subject to the 30-day policy. These invoices are to be paid as soon as administratively possible after NEHII receives reimbursement.

Invoices will not normally be paid until the responsible Chief, Director, or the Office Manager affirms via OneDesk that the goods or services were received in full and were satisfactory. This will be defined as operational approval. Exceptions will be made for certain prepaid expenses (such as insurance premiums) and when necessary to encumber federal funds to avoid their expiration. Approval of the Director of Grants and Contracts Management and the Chief Executive Officer is necessary to encumber federal funds.

Once operational approval has been approved, invoices are to be paid in accordance with the timeframe above, applying the financial approval requirements detailed in the Division of Responsibilities section.

Disputed invoices are not subject to these requirements. In no case should invoices be paid before NEHII agrees the invoiced items or services are satisfactory.

## Payroll

Department chiefs review and approve timecards on a weekly basis and the approved hours are the basis for the time component of the payroll calculation. The Chief Financial Officer reviews and approves the Chief Executive Officer's timecard on a weekly basis. The pay rates used to prepare payroll are based on signed memos from the Chief Executive Officer. The salary for the Chief Executive Officer is based on a signed memo from the Board President. All pay rates in the third-party software are maintained and updated by the Human Resources Generalist.

Initial payroll processing is reviewed and initiated by the Human Resources Manager, who uses software provided through a third-party vendor, ADP. In the absence of the Human Resources Manager, the Human Resources Generalist initiates processing. The Chief Financial Officer verifies payroll amounts before granting approval for final processing. In the absence of the Chief Financial Officer, the Chief Executive Officer grants final approval.

## Expense Reimbursements

Employees will be reimbursed for ordinary and necessary expenses in connection to NEHII business when adequately accounted to NEHII. See IRS Publication 463 Travel, Gift, and Car Expenses for the applicable year for details, including the mileage reimbursement rate for employee-owned vehicles.

Expense reimbursement reports for employees are to be submitted no later than the 10<sup>th</sup> day of the month subsequent to when the expense was incurred to ensure for their inclusion in financial reports on a timely basis.

Expense reimbursement reports for board members and others are to be requested, but are not required, in the same timeframe as above.

Reimbursement will not occur if the expense reimbursement request is turned in greater than 60 days after the expense was incurred.

Expense reports are reviewed and approved by the Chief Financial Officer. Expense reimbursements for the Chief Financial Officer are reviewed and approved by the Chief Executive Officer.

Expense reports must be supported by receipts when applicable and include the project(s) and/or purpose to which the expenses relate to support business connection. Failure to provide required information or support may result in the denial of reimbursement.

Expense reimbursements will be paid out within 15 business days after approval.

Expense reimbursement checks that expire due to employee disregard will not be re-issued. The Accounts Payable accountant will reach out to employees 30 days before the expiration date to ensure the check was received and will re-issue the check if necessary due to loss.

## Cash/Check Receipts

The receipt of cash should be exceedingly rare. Whenever cash is received a receipt should be given to the payer with a reference to the invoice number and/or the reason it was received. A copy of the receipt must be made and retained in SharePoint for deposit documentation.

When checks are received, they should immediately be restrictively endorsed for deposit only into the appropriate NEHII account. Checks are logged and scanned into OneDesk and forwarded to the Accountant II who prepares the bank deposit and enters the amounts into the General Ledger (GL). The Accounting Clerk or Office Manager takes the deposit to the bank.

## Bank Reconciliations

Bank Statements are forwarded to the Chief Financial Officer unopened.

Upon opening the statements, the Chief Financial Officer reviews them for unusual items or changes. The Chief Financial Officer compares selected deposits on the

bank statement to the copy of cash and check receipts logs and reviews any account transfers.

The bank statements are to be reconciled by the Director of Accounting on a monthly basis no more than one week after receipt. The general ledger and the reconciled bank statements will be adjusted to agree monthly. Any adjustments will be reviewed and approved by the Chief Financial Officer before posting.

## End of Month Accounting

The Director of Accounting prepares the monthly financial statements. The Chief Executive Officer reviews and the Chief Financial Officer reviews and approves the financial statements before being sent to the Board of Directors. The financial statements should be to the Chief Financial Officer at least four days prior, and to the Chief Executive Officer two days prior to the publishing of Board packets.

The Board of Directors approves the monthly financial statements.

## End of Year Accounting

The Director of Accounting prepares the year-end financial statements.

The Director of Accounting is responsible for preparing for the annual financial audit and for working with the outside accountants to complete the audit.

The Chief Executive Officer reviews and the Chief Financial Officer reviews and approves the financial statements before being sent to the Board of Directors. The financial statements should be to the Chief Financial Officer at least 10 days prior, and to the Chief Executive Officer four days prior to the publishing of Board packets.

The Board of Directors approves the year-end financial statements and the associated footnotes.

## Cost Allocations

NEHII is required to follow various guidelines for allocating costs which benefit more than one program or grant. It is the policy of NEHII to comply with the requirements of all grant contracts and the Federal Acquisition Regulation.

## Investments

Cash not needed for immediate working capital will be transferred to interest bearing investments, unless the funds are designated for a particular purpose, such as a pass-through payment to a grant sub-recipient.

## **Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider**

NEHII will maintain a money market account at the same bank where the checking accounts are maintained. Certificates of deposit may also be used to invest excess cash. The Chief Financial Officer will initiate the transfer of funds setting up new certificates of deposit based on the projected cash flow requirements and budgets of all NEHII entities.

The Board of Directors must approve any investments beyond money market and certificates of deposit taking into consideration the recommendations from the NEHII Foundation, Inc.'s Investment Committee and within the parameters of the NEHII Investment Policy.

### **Debt**

Board approval is required for incurring any debt of NEHII other than operating trade payables and budgeted payroll payables. The Chief Financial Officer will be authorized to negotiate such debt as needed by the Board of Directors.

Any loan covenants and restrictions will be reported to the Board when the debt is authorized. The Chief Financial Officer will periodically review these covenants and report to the Chief Executive Officer if there are any violations or potential violations of the covenants.

The Chief Executive Officer and Board President or Treasurer will sign any debt agreements after receiving full Board approval.

### **Reserves and Designated Funds**

NEHII will target to build and maintain an operating reserve to assist in maintaining financial stability. The reserve may be invested consistent with the investment policy of NEHII.

The Board of Directors may designate portions of the net assets of NEHII for specific purposes.

### **Internal Controls and Financial Audit**

The review of internal controls and the annual audit are two of the most important procedures the Board has for fulfilling its fiduciary responsibilities to NEHII.

Internal controls pertaining to the accounting records are established by the Chief Executive

## **Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider**

Officer, Chief Financial Officer and Board Treasurer in consultation with the Director of Accounting.

The Board of Directors selects the public accounting firm which will perform the year-end financial audit. The financial audit report is presented to the Board of Directors, who have the authority to approve the audit.

### **Credit Card Policy**

All employees who are authorized to carry an organization credit card will be held personally responsible for any charge that is deemed personal or unauthorized.

Unauthorized use of the credit card includes: personal expenditures of any kind; expenditures which have not been properly authorized; meals, entertainment, gifts, or other expenditures which are prohibited by budgets, laws and regulations, and the entities from which NEHII receives funds.

Employee credit card use is monitored monthly through the credit card statement reconciliation process. The Chief Financial Officer reviews the credit card usage for all cards assigned to other employees. The Human Resources Manager reviews the credit card usage for the card assigned to the Chief Financial Officer.

### **Compliance**

In order to continue receiving government grants and restricted donations, NEHII must have systems in place to ensure compliance with the restrictions imposed by those grants and restricted donations.

The Director of Grants and Contracts Management will be responsible for overseeing the compliance with all applicable grant restrictions.

The Chief Financial Officer will be responsible for communicating the nature of all donor restrictions to the Director of Accounting. This information will be used to ensure that the General Ledger restricted donations account will reflect the restricted donations and the spending of those restricted amounts as appropriate.

## Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider

### Budgeting

The Board of Directors is responsible for guiding the budget process and for approval of the annual budget.

The Chief Financial Officer will be responsible for preparing the proposed budget, with guidance from the Chief Executive Officer and support from the Director of Accounting and Director of Grants and Contracts Management.

### Software Authorization and Backup

The accounting software will have access controlled by passwords. The Director of Accounting will be given a complete system password and will control which other personnel will be given passwords.

The accounting software will be backed up weekly. The Director of Accounting is responsible for ensuring the backup is completed.

The Director of Accounting is responsible for maintaining the disaster recovery plan for the accounting software and for testing the plan at least once annually.

### Record Retention

Record retention is governed by various rules, statutes of limitations and common sense. Certain documents must be retained indefinitely, while others may have little use after a year. In all cases, records will be maintained at least as long as any statute of limitations applies.

The Director of Accounting is responsible for the record retention schedule. The Chief Financial Officer must grant permission to discard records in case an exception to the standard schedule is necessary.

### Maintenance of Accounting Policies Manual

The accounting policies manual is critical to the accounting function of NEHII.

The Director of Accounting is responsible for maintaining the manual. A review of the manual must be completed each 4<sup>th</sup> quarter in connection with the development of the subsequent

## **Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider**

fiscal year's budget.

All proposed changes must be approved by the Board of Directors. The policies manual will be dated with each approved revision.

### **Preparation of Tax Returns**

Tax-exempt organizations of NEHI are required to file annually to the IRS the Form 990, Return of Organization Exempt from Income Tax, including the required Schedules. All other organizations will file the appropriate federal tax form (Form 1120, Form 1065, etc.) based on the type of organization.

The preparation of the tax filings will generally be contracted out to an independent accounting firm. The Director of Accounting will be responsible for providing the information needed to prepare the returns. The Chief Financial Officer will review all reports prior to filing them to ensure that they are accurate. The federal annual returns will also be reviewed by the Chief Executive Officer before filing.

The Form 990 will be presented to the Board of Directors and/or the Executive and Finance Committee to review before filing. After review, the Chief Financial Officer will sign and work with the independent accounting firm to file before the deadline.

NEHI will file all appropriate federal and state government filings including but not limited to payroll tax, sales tax, property tax, Form 1099, Form W-2, Form 1120N, Form 990-T.

For those tax filings that are required under the law to be available to the public for review after filing, NEHI will make available upon request.

### **Property and Equipment Inventory**

An inventory of all property and equipment will be maintained. The inventory document will contain sufficient information for insurance, tax returns and grant requirements.

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

## Grants and Contracts

Grant and contract billings will be prepared and filed timely in accordance with the grant or contract requirements. Monthly invoicing is the preferred interval. Adequate documentation will be maintained to support all billings.

## Revision Tracking

<b>Date</b>	<b>Version</b>	<b>Changes</b>	<b>Performed by</b>
2/23/21	2	Expense reimb policy, CFO Title change	Zac Roberts



**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

**Attachment G  
Patient Education-English**

## Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider

### OPTING IN OR OUT IS YOUR CHOICE

If your provider is a CyncHealth participant, your information will automatically be included in CyncHealth. Though your participation in the HIE is completely voluntary, it is greatly encouraged for your own benefit. CyncHealth improves communication among your providers by ensuring care teams have the right information at the point of care. The more information your doctor has about you, the more effectively he or she can treat you—resulting in smooth exchanges of information that promote a seamless—and cost-effective—patient experience.

If you do not wish to share your health records with your care providers, you can opt out via one of two ways:

- Call CyncHealth support at 402-506-9900, ext. 1; or
- Go to [www.cynchealth.org](http://www.cynchealth.org) and complete the form under the tab, Opt In/Opt Out

Opting out will remove your information from viewing by providers in the CyncHealth query except for your name, address and opt-out status. It will not affect what your doctors have access to in their electronic medical records, and it will not be a condition to receiving care. It also won't affect other sharing of health information via fax, phone or other means between your providers, health insurers or public health agencies. It may, however, affect the comprehensiveness of information your provider has available to effectively provide you care.

You can opt back in at anytime by calling CyncHealth support at 402-506-9900 ext. 1 or visiting [www.CyncHealth.org](http://www.CyncHealth.org).

### ABOUT CYNCHHEALTH

CyncHealth was sponsored by Nebraska health care providers and insurance organizations to serve as Nebraska's regional HIE. Through the HIE, participating providers and health insurers can see certain health, demographic and payment information (your health information) in each other's records. They can use this information for treatment and payment purposes.

In addition to serving as the region's HIE, CyncHealth also partners with the Nebraska Department of Health and Human Services to administer the Prescription Drug Monitoring Program (PDMP). The PDMP provides a comprehensive query-based medication history of all dispensed prescriptions in Nebraska, as well as mail order pharmacies dispensing prescriptions to Nebraska zip codes.

CyncHealth also supports the Nebraska Healthcare Collaborative, a nonprofit promoting health data science throughout the state to help providers make data-driven decisions that will lower costs and improve health outcomes for the people of Nebraska. CyncHealth supplies the Collaborative de-identified information collected from many patient records to discover new ways to improve health care for everyone.

---

*Note: CyncHealth and the participating providers and health insurers have the right to change policies and the information in this brochure over time. Visit [www.CyncHealth.org](http://www.CyncHealth.org) for the most current version and information.*

### CONTACT

402-506-9900 ext. 1 | PO Box 27842 | Omaha, NE 68127



Sharing Information  
for better health care

[www.cynchealth.org](http://www.cynchealth.org)

## Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider

### WHAT IS A HEALTH INFORMATION EXCHANGE?

Health information exchanges (HIEs) provide the capability to electronically move clinical information among disparate health care information systems and maintain the meaning of the information being exchanged. The goal of HIEs is to facilitate access to and retrieval of clinical data to provide safe, more timely, efficient, effective, equitable, patient-centered care. HIEs are also used by public health authorities to assist in analyzing the health of populations.

### HOW SHARING HEALTH INFORMATION CAN IMPROVE PATIENT CARE

Health care providers need your health information to accurately diagnose and treat you. Each of your providers may have different portions of your medical record. If they can access each other's records and see more complete health information, they can provide you with better care. Sharing your health information can also help reduce your costs by eliminating unnecessary duplication of tests and procedures.

### HOW IS YOUR INFORMATION SHARED & WHO HAS ACCESS?

Health care providers have always shared health records. Most recently, faxes and postal mail were the most popular methods of sharing, and sharing was usually done on a case-by-case basis.



HIEs like CyncHealth allow health care providers to share the health records of all of their patients through security protocols to ensure privacy.

CyncHealth automates the task of locating, making the process of sharing health information more efficient. It also allows one participant (i.e. a doctor) to locate records from another participant (i.e. a hospital) in a matter of minutes. This can be critical in an emergency and may result in your providers having more complete and accurate information about you.

Participating providers (i.e. doctors, hospitals and pharmacies), health insurers and community public health agencies will have access to your health information for treatment, payment and operations (i.e. public health reporting) purposes on a need-to-know basis. CyncHealth will also have access to provide support, and medical researchers may have access to certain de-identified health information.

### TYPES OF INFORMATION SHARED & PROTECTING YOUR PRIVACY

CyncHealth follows all federal (42 CFR Part II) and state privacy laws in the reporting of availability of data. Patient data shared may include medication and immunization history, lab and x-ray results, transcribed diagnostic and treatment records, records of allergies and drug reactions and other transcribed clinical reports created after January 1, 2013, but only if the provider who has the information is a participating provider and makes the information available.

CyncHealth and the participating providers and health insurers use a combination of safeguards to protect your health information:

- Privacy and security safeguards include encryption, password protection and the ability to track every viewer's usage of the system
- Administrative safeguards include written policies controlling access to information through CyncHealth

All participating providers and health insurers must agree to follow these policies, in addition to being regulated by federal and state privacy laws. They must also have their own policies and other safeguards in place, including policies to train their staff and limit access to those with a need to know the information.

You can learn more about how your privacy is protected by visiting:  
[www.CyncHealth.org/privacy-security](http://www.CyncHealth.org/privacy-security)

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

**Attachment H  
Patient Education-Spanish**

## Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider

### ACEPTAR PARTICIPAR O NO PARTICIPAR ES SU DECISIÓN

Si su proveedor es un participante de la CyncHealth, su información se incluirá automáticamente en la CyncHealth. Aunque su participación en los HIE es completamente voluntaria, se recomienda mucho para su propio beneficio. La CyncHealth mejora la comunicación entre sus proveedores al garantizar que los equipos de atención tengan la información correcta en el punto de atención. Cuanta más información tenga su médico sobre usted, más eficazmente podrá tratarlo, lo que dará como resultado intercambios de información sin problemas que promoverán una experiencia del paciente eficiente y económica.

Si no desea compartir sus expedientes médicos con sus proveedores de atención, puede optar por una de estas dos opciones:

- Llame al soporte de la CyncHealth al 402-508-9900, ext. 1; o
- Vaya a [www.cynchealth.org](http://www.cynchealth.org) y complete el formulario bajo la pestaña, Opt-In/Opt-Out (Aceptar Participar o No Participar)

Al decidir no participar se eliminará su información y los proveedores no la podrán ver al consultar la CyncHealth, excepto su nombre, dirección y si decidió participar o no en la iniciativa. Esto no afectará a lo que sus médicos tienen acceso en sus registros médicos electrónicos, y no será una condición para recibir atención. Tampoco afectará el intercambio de información médica por fax, teléfono, o otros medios entre sus proveedores, seguros médicos, o agencias de salud pública. Sin embargo, puede afectar la extensión de la información que su proveedor tiene disponible para brindarle atención de manera efectiva.

Puede volver a participar en cualquier momento llamando al soporte de la CyncHealth al 402-508-9900 ext. 1 o visitando [www.cynchealth.org](http://www.cynchealth.org).

### SOBRE LA CYNCHHEALTH

La CyncHealth fue patrocinada por proveedores de atención médica de Nebraska y organizaciones de seguros para desempeñarse como los Intercambios de Información Médica (HIE, por sus siglas en inglés) regional de Nebraska. A través de los HIE, los proveedores participantes y seguros médicos pueden ver cierta información médica, demográfica y de pago (su información médica) en los expedientes de las personas. Pueden usar esta información para fines de tratamiento y pago.

Además de desempeñarse como los HIE de la región, la CyncHealth también se asocia con el Departamento de Salud y Servicios Humanos de Nebraska para administrar el Programa de Monitoreo de Medicamentos Recetados (PDMP). El PDMP proporciona un historial completo de medicamentos basado en consultas de todas las recetas despachadas en Nebraska, así como farmacias ofreciendo pedidos por correo que despachan las recetas a los códigos postales de Nebraska.

La CyncHealth también apoya la Nebraska Healthcare Collaborative, una organización sin fines de lucro que promueve la ciencia de datos médicos en todo el estado para ayudar a los proveedores a tomar decisiones basadas en datos que reducirán los costos y mejorarán los resultados de la salud para la gente de Nebraska. La CyncHealth proporciona la información no identificada de la colaboración recopilada de muchos expedientes de pacientes para descubrir nuevas formas de mejorar la atención médica para todos.

*Nota: La CyncHealth y los proveedores y seguros médicos participantes tienen derecho a cambiar las pólizas y la información de este folleto con el tiempo. Visite [www.cynchealth.org](http://www.cynchealth.org) para obtener la versión y la información más actual.*

### CONTACTO

402-508-9900 ext. 1 | PO Box 27842 | Omaha, NE 68127



Compartiendo información  
para una mejor  
atención médica

[www.cynchealth.org](http://www.cynchealth.org)

## Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider

### WHAT IS A HEALTH INFORMATION EXCHANGE?

Health information exchanges (HIEs) provide the capability to electronically move clinical information among disparate health care information systems and maintain the meaning of the information being exchanged. The goal of HIEs is to facilitate access to and retrieval of clinical data to provide safe, more timely, efficient, effective, equitable, patient-centered care. HIEs are also used by public health authorities to assist in analyzing the health of populations.

### HOW SHARING HEALTH INFORMATION CAN IMPROVE PATIENT CARE

Health care providers need your health information to accurately diagnose and treat you. Each of your providers may have different portions of your medical record. If they can access each other's records and see more complete health information, they can provide you with better care. Sharing your health information can also help reduce your costs by eliminating unnecessary duplication of tests and procedures.

### HOW IS YOUR INFORMATION SHARED & WHO HAS ACCESS?

Health care providers have always shared health records. Most recently, faxes and postal mail were the most popular methods of sharing, and sharing was usually done on a case-by-case basis.



HIEs like CyncHealth allow health care providers to share the health records of all of their patients through security protocols to ensure privacy.

CyncHealth automates the task of locating, making the process of sharing health information more efficient. It also allows one participant (i.e. a doctor) to locate records from another participant (i.e. a hospital) in a matter of minutes. This can be critical in an emergency and may result in your providers having more complete and accurate information about you.

Participating providers (i.e. doctors, hospitals and pharmacies), health insurers and community public health agencies will have access to your health information for treatment, payment and operations (i.e. public health reporting) purposes on a need-to-know basis. CyncHealth will also have access to provide support, and medical researchers may have access to certain de-identified health information.

### TYPES OF INFORMATION SHARED & PROTECTING YOUR PRIVACY

CyncHealth follows all federal (42 CFR Part II) and state privacy laws in the reporting of availability of data. Patient data shared may include medication and immunization history, lab and x-ray results, transcribed diagnostic and treatment records, records of allergies and drug reactions and other transcribed clinical reports created after January 1, 2013, but only if the provider who has the information is a participating provider and makes the information available.

CyncHealth and the participating providers and health insurers use a combination of safeguards to protect your health information:

- Privacy and security safeguards include encryption, password protection and the ability to track every viewer's usage of the system
- Administrative safeguards include written policies controlling access to information through CyncHealth

All participating providers and health insurers must agree to follow these policies, in addition to being regulated by federal and state privacy laws. They must also have their own policies and other safeguards in place, including policies to train their staff and limit access to those with a need to know the information.

You can learn more about how your privacy is protected by visiting:  
[www.CyncHealth.org/privacy-security](http://www.CyncHealth.org/privacy-security)

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

**Attachment I  
User Audit Request Form**

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

**CyncHealth User Audit Request**

As provided in the CyncHealth Data Sharing Participation Agreement, CyncHealth Participants are responsible for ensuring appropriate administrative, physical, and technical safeguards are in place to protect the System and information accessible through the system, as well as keeping current all Authorized Users' account access to the System. To assist in performing compliance reviews, CyncHealth can provide a comprehensive audit for a specified period of time of Authorized User access to the System upon request from Participant.

A Participant's Privacy Officer requesting data shall complete this form and submit to [support@cynchealth.org](mailto:support@cynchealth.org). Upon receipt, an informational copy of the completed form will be provided to an appropriate CyncHealth employee who will contact you with any questions and next steps.

Date of Request:	
Name of Requestor and Title:	
Date Range for Request:	
Entity Participant Name:	

As provided in the CyncHealth Data Sharing Participation Agreement, CyncHealth may change its Miscellaneous Charges upon thirty (30) days' written notice to Participant. *This form shall be considered official notice that the submitted User Audit request will constitute a change in Miscellaneous Charges.* By submitting this form the Requester understands and acknowledges that CyncHealth may charge Participant for the processing of this user audit. The individual executing this represent and warrant that they are authorized to commit Participant to paying for services under the Participation Agreement.

\_\_\_\_\_  
Printed name & title

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date



**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

**Attachment J  
Audit Standard Operating Procedure**

## **Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider**

### **AUDIT REQUEST STANDARD OPERATING PROCEDURE**

#### **Receive Request**

- If request comes to team member, forward email request to Support

#### **Support will create Jira ticket w/ assignment**

- Support may send User Audit Request Form to facility with instructions for Facility Privacy Officer to complete the form and submit back to [support@cynchelath.org](mailto:support@cynchelath.org).
- Assign to **Legal**
- Include facility name, contact information of requester, any documents attached to email, and explanation of assignment determination.
- Tag the following individuals: **Meghan Chaffee, Bob Kelly, Tamara Stepanek, Robert Wagner**

#### **Legal (Privacy Officer) will verify the request before beginning any audit process.**

CyncHealth will only process a request for user audits after all the following conditions have been met in full:

- Disclosure of Authorized User information is authorized in accordance with CyncHealth privacy and security policies;
- The identity of the requestor has been validated in accordance with the relevant policies and regulations;
- A properly complete form has been submitted;
- Confirm understanding the audit may require a fee in addition to usual participation and miscellaneous fees as outlined in Participation Agreement; and,
- Name, title and authority to request a user audit of the Requester (Participant's designated Privacy Officer) is verified.

#### **Legal will request audit of Participant's Authorized Users' access of the system from ISC.**

- Confirm request and provide timeline of return to Participant
- If any associated fees, provide Participant reminder of cost

#### **Upon return of audit from ISC Legal will share with CISO for secure sharing and will email Participant instructions for viewing their records.**

- Include Finance in delivery email to trigger generation and sending of invoice for audit request if applicable.

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

**Attachment I  
Subcontractor BAA**

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

**Nebraska Health Information Initiative, Inc., DBA CyncHealth  
BUSINESS ASSOCIATE  
SUBCONTRACTOR AGREEMENT**

**THIS SUBCONTRACTOR AGREEMENT** (“Agreement”) is between Nebraska Health Information Initiative, Inc., DBA CyncHealth (“Business Associate”) and [name of vendor] (“Subcontractor”). This Agreement is effective as of the Effective Date set forth below.

1. **Definitions.** Terms used but not otherwise defined in this Agreement shall have the meaning ascribed in section 160.103, 164.501, or elsewhere, in the Regulations.
  - a. **“ePHI”** means PHI that is maintained or transmitted in electronic media.
  - b. **“Breach”** means, with respect to PHI, the impermissible acquisition, access, use or disclosure of Unsecured PHI which compromises the security or privacy of the PHI.
  - c. **“Subcontractor Functions”** means all functions performed by Subcontractor under one or more Service Agreements on behalf of Business Associate which involve the creation of, access to, use or disclosure of PHI by Subcontractor or its agents or subcontractors.
  - d. **“HIPAA”** means the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d to 1320d-7, and future amendment thereto and the Regulations issued thereunder.
  - e. **“PHI”** means protected health information as defined in the Regulations, which is created, obtained or used by Subcontractor in the performance of one or more Subcontractor Functions for Business Associate.
  - f. **“Regulations”** means the final Regulations implementing the privacy and security provisions of HIPAA as amended from time to time. The Regulations are presently codified at 45 C.F.R. Parts 160, 162 and 164.
  - g. **“Services Agreement(s)”** or **“Agreement”** means all agreements, whether written or oral, and whether now in effect or hereafter entered into, between Business Associate and Subcontractor for the performance of Subcontractor Functions by Subcontractor. Existing Services Agreement(s) are listed on attached Exhibit A.
  - h. **“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.
  - i. **“Unsecured PHI”** means PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals by one or more of the methods outlined by the

## Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider

Department of Health and Human Services in 74 Fed. Reg. 19006 (2009) (to be codified at 45 C.F.R. §160 and §164).

2. **Purpose.** CyncHealth is a Business Associate under HIPAA to various covered entities (“Participants”) participating in the electronic exchange of information through the record locator service and other data exchange services provided by CyncHealth (“System”). Business Associate requires certain services of Subcontractor as detailed in the Services Agreement (“Subcontractor Functions”), which involves access to PHI of multiple Participants. HIPAA requires Business Associate to obtain satisfactory written contractual assurances from its subcontractors before furnishing them with PHI or permitting them to obtain or create PHI to perform functions on its behalf. This Agreement is entered into to provide Business Associate with the contractual assurances required under HIPAA.

3. **Permitted Uses and Disclosures of PHI.** Subcontractor shall only use and disclose PHI for the following purposes:

a. To perform Subcontractor Functions.

b. As needed for the proper management and administration of Subcontractor and to carry out the legal responsibilities of Subcontractor.

4. **Special Conditions on Disclosure for Subcontractor’s Purposes.** Before Subcontractor may *disclose* PHI to another party for a reason described in subparagraph 3b, one of the following two conditions must be met; either –

a. the disclosure must be *required by law*; or

b. Subcontractor must obtain *reasonable assurances* from the person to whom the PHI is disclosed that such person will safeguard the PHI and further use and disclose it only as required by law or for the purpose for which Subcontractor disclosed it to such person; and such person must agree in writing to notify Subcontractor of any instances of which it is aware in which the confidentiality of the PHI has been breached.

5. **Assurances of Subcontractor.** As an express condition of performing Subcontractor Functions, Subcontractor agrees to:

a. Comply with the requirements of Title XII, Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act, codified at 42 U.S.C. §§ 17921-17954, which are applicable to Subcontractor, and comply with all regulations issued by the Department of Health and Human Services (HHS) to implement HITECH, as of the date by which Subcontractor is required to comply with HITECH and the related regulations. Such requirements are hereby incorporated by reference into this Subcontractor Agreement.

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

- b. Use and disclose PHI only as permitted or required by this Agreement, or as otherwise required by law. Subcontractor shall not use or disclose information in a manner that would violate any applicable law if done by Business Associate.
- c. Use appropriate safeguards to prevent use or disclosure of PHI other than as provided for in this Agreement.
- d. Report to Business Associate's designated privacy official, without unreasonable delay but in no event more than five (5) business days of discovery by Subcontractor, any acquisition, access, use or disclosure of PHI not provided for in this Agreement or not permitted under the Regulations, including any impermissible access, acquisition, use or disclosure that is a Breach of Unsecured PHI, together with any remedial or mitigating action taken or proposed to be taken with respect thereto. Subcontractor shall conduct a risk assessment with respect to any impermissible access, acquisition, use or disclosure to determine if there is a significant risk of financial, reputational or other harm to the individual whose PHI was impermissibly acquired, accessed, used or disclosed. Subcontractor shall notify Business Associate of any such impermissible access, acquisition, use or disclosure, including the following information in such notice:
- i. A brief description of how the impermissible access, acquisition, use or disclosure occurred and how and when it was discovered.
  - ii. A description of whether Unsecured PHI was involved in the impermissible access, acquisition, use or disclosure, and the results of Subcontractor's risk assessment.
  - iii. The steps Subcontractor is taking to further investigate the impermissible access, acquisition, use or disclosure, to mitigate losses, and to protect against further impermissible access, acquisition, use or disclosure.
- Subcontractor shall cooperate with Business Associate in mitigating any harmful effects of any such impermissible access, acquisition, use or disclosure, and in making any required notification to individuals in the case of a Breach as determined by Business Associate. Subcontractor shall pay for the costs of such mitigation and notification if the Breach was due to a violation of this Agreement by Subcontractor, or the negligent or intentional actions of Subcontractor.
- e. Provide individuals with access to and copies of PHI maintained by Subcontractor in designated record sets, and limit fees for access and copying, all in accordance with Business Associate's obligations to individuals under 45 C.F.R. § 164.524.
- f. Notify Business Associate within three (3) business days of any request by individuals to amend PHI maintained by Subcontractor in designated record sets, direct the requesting

## **Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider**

individual to Business Associate for handling of such request, cooperate with Business Associate in the handling of such request, and incorporate any amendment accepted by Business Associate in accordance with §164.526 of the Regulations. Subcontractor is not authorized to independently agree to any amendment of PHI.

g. Maintain a record of those disclosures of PHI by Subcontractor or its agents or subcontractors which are subject to the individual's right to an accounting under § 164.528 of the Regulations and report such disclosures to Business Associate within five (5) business days of request by Business Associate in a form permitting Business Associate to respond to an individual's request for an accounting.

h. Make its internal practices, books and records relating to the use and/or disclosure of PHI available to the Secretary of HHS or his or her designees for purposes of determining Business Associate's compliance with the Regulations.

i. Return to Business Associate or destroy (and not retain a copy) all PHI in its possession, upon the termination of the Services Agreement or as soon as such PHI is no longer needed by Subcontractor to perform its responsibilities hereunder, whichever comes first, and require its agents and subcontractors to do likewise. To the extent that return or destruction is not feasible, the protections of this Agreement shall remain in effect for so long as Subcontractor or its agents or subcontractors have possession of or access to such PHI, and Subcontractor agrees to limit further uses and disclosures of the PHI to those purposes which make return or destruction infeasible.

j. Ensure that all agents and subcontractors who will create, receive, use or disclose PHI to perform a Subcontractor Function under this Agreement agree in writing to adhere to the same restrictions and conditions on the use and/or disclosure of PHI that apply to Subcontractor.

k. Ensure that all other agents and contractors of Subcontractor who have access to PHI to perform other services (other than Subcontractor Functions) to Subcontractor agree in writing to take reasonable steps to safeguard the privacy of PHI.

l. Comply with any voluntary restriction on use or disclosure of PHI accepted by Business Associate under § 164.522(a) of the Regulations which is properly communicated to Subcontractor.

m. Comply with any reasonable requests by individuals under § 164.522(b) of the Regulations to receive communications of PHI by alternative means or at alternate locations when communicated to Subcontractor by Business Associate or directly by the individual.

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

n. Limit the use and disclosure of PHI for purposes described in this Agreement to the minimum necessary to perform the required function. Subcontractor shall comply with any additional requirements for the determination of minimum necessary as are required from time to time by the Regulations, as amended.

6. **Security Assurances of Subcontractor.** If Subcontractor will create, receive, maintain or transmit ePHI on behalf of Business Associate, it further agrees to:

a. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of ePHI.

b. Ensure that any agent, including a subcontractor, to whom it provides ePHI, or with whom it contracts to create, receive, maintain or transmit ePHI, agrees to implement reasonable and appropriate safeguards to protect such ePHI.

c. Report to Business Associate any Security Incident of which Subcontractor becomes aware.

d. Comply with any other required provision of the Regulations, as amended by the HITECH Act.

7. **Responsibilities of Business Associate.** Business Associate agrees to:

a. Notify Subcontractor promptly if Business Associate agrees to any voluntary restrictions on the use or disclosure of PHI which will affect Subcontractor's use or disclosure of PHI under the Services Agreement.

b. Notify Subcontractor of any reasonable requests by individuals under §164.522(b) of the Regulations to receive communications of PHI by alternative means or at alternative locations, if such requests will affect Subcontractor's services.

c. Provide Subcontractor with a copy of any amendment to PHI which is accepted by Business Associate under §164.526 of the Regulations which Business Associate believes will apply to PHI maintained by Subcontractor in designated record sets.

8. **Supervening Law.** Upon the enactment of any law or regulation affecting the use or disclosure of PHI, or the publication of any decision of a court of the United States or of this state relating to any such law, or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, Business



## Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider

Associate may, by written notice to Subcontractor, amend this Agreement in such manner as it determines necessary to comply with such law or regulation. If Subcontractor disagrees with any such amendment, it shall so notify Business Associate in writing within thirty (30) days of Business Associate's notice. If the parties are unable to agree on an amendment within thirty (30) days thereafter, either party may terminate the Services Agreement on not less than thirty (30) days' written notice to the other. If not so terminated, the amendment or amendments proposed by Business Associate shall become effective.

9. **Identity Theft Prevention Program.** Subcontractor acknowledges that Business Associate has adopted, or will adopt, an Identity Theft Prevention Program as required under 16 C.F.R. Part 681 ("Red Flags Rule") for certain covered accounts that may be accessed in accordance with the Service Agreement. Subcontractor acknowledges that it may be a Service Provider under Business Associate's Identity Theft Prevention Program. Accordingly, to the extent Subcontractor is a Service Provider as that term is defined in the Red Flags Rule, Subcontractor will conduct its activities in accordance with reasonable policies and procedures to detect, prevent and mitigate identity theft. Subcontractor shall report to Business Associate's compliance officer, within three (3) business days of a reasonably confirmed incidence of identity theft involving Business Associate's covered accounts, together with any remedial or mitigating action taken or proposed to be taken with respect thereto. Subcontractor shall cooperate with Business Associate in mitigating any harmful effects of any such activity.

10. **Term and Termination.**

a. **Term.** This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, including return or destruction of all PHI in Subcontractor's possession (or in the possession of Subcontractor's agents and subcontractors), unless sooner terminated as provided herein. It is expressly agreed that the terms and conditions of this Agreement designed to safeguard PHI shall survive expiration or other termination of the Services Agreement and shall continue in effect until Subcontractor has performed all obligations under this Agreement.

b. **Termination by Business Associate.** Business Associate may immediately terminate the Services Agreements, if Business Associate makes the determination that Subcontractor has breached a material term of this Agreement. Alternatively, Business Associate may choose to provide Subcontractor with written notice of the existence of an alleged material breach, and afford Subcontractor an opportunity to cure the alleged material breach upon mutually agreeable terms. Failure to take reasonable steps to cure the breach is grounds for the immediate termination of this Agreement.

c. **Termination by Subcontractor.** If Subcontractor determines that Business Associate has breached a material term of this Agreement, Subcontractor shall notify Business Associate and provide Business Associate an opportunity to cure the alleged material breach upon

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

mutually agreeable terms. Failure of Business Associate to take reasonable steps to cure the breach is grounds for the immediate termination of this Agreement.

d. **Return/Destruction infeasible.** In the event that Subcontractor determines that returning or destroying the PHI is infeasible, Subcontractor shall provide to Business Associate notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Subcontractor shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Subcontractor maintains such PHI.

11. **Miscellaneous.**

a. **Business Associate.** For purposes of this Agreement, and as applicable to the Subcontractor Functions of Subcontractor under all Service Agreements covered by this Agreement, references to Business Associate shall include the named Business Associate and all other entities covered by a joint Notice of Privacy Practices with Business Associate, whether as part of an affiliated Business Associate or an organized health care arrangement.

b. **Survival.** The respective rights and obligations of Subcontractor and Business Associate hereunder shall survive termination of this Agreement according to the terms hereof and the obligations imposed on Business Associate under HIPAA.

c. **Interpretation; Amendment.** This Agreement shall be interpreted and applied in a manner consistent with Business Associate's obligations under HIPAA. Except as provided in Section 8 of this Agreement, all amendments shall be in writing and signed by both parties, except that this Agreement shall attach to additional Services Agreements entered into between the parties in the future without the necessity of amending this Agreement each time. This Agreement is intended to cover the entire Subcontractor *relationship* between the parties, as amended, from time to time, through Services Agreements or other means.

d. **Waiver.** A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

e. **No Third-Party Beneficiaries.** Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies or obligations.

*Signatures on next Page*

**Application for Certificate of Authority to Operate as a  
Health Information Exchange Service Provider**

This Agreement is effective \_\_\_\_\_ 2021.

**IN WITNESS WHEREOF**, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

Business Associate: Nebraska Health  
Information Initiative, Inc., DBA CyncHealth

**Subcontractor:**

Signature: \_\_\_\_\_

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date Signed: \_\_\_\_\_

Date Signed: \_\_\_\_\_