



## Response to CyncHealth HIO Certification Application Status-Final Notice


### Attestation

CyncHealth attests to the accuracy of responses provided as part of the original application and Attachment A, Attachment B, and Attachment C, with the exception of updates identified below.


### Application for Certificate of Authority to Operate as a Health Information Exchange Service Provider Health Information Organization (HIO)

#### Section VIII: Meaningful Use Transactions

1. Electronic Prescribing	Currently Offered	Plan to Offer in next 12 months
1.a. New Prescription (Provider to Pharmacy) (NEWRX)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
1.b. Fill status notification (Pharmacy to Provider) (RXFILL)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
1.c. Refill Renewal Request (Pharmacy to Provider) (REFREQ)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
1.d. Refill Renewal Response (Provider to Pharmacy) (REFRES)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
1.e. Cancel messages (CANRX, CANRES)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
1.f. Prescription Change Request (RXCHG)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
1.g. Prescription Change Response (CHGRES)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
1.h. Medication History Request (RXHREQ)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
1.i. Medication History Response (RXHRFS)	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

 402-506-9900

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

 CyncHealth  
PO Box 27842  
Omaha, NE 68127



CyncHealth is NOT currently supporting electronic prescribing in Minnesota (i.e., NO to 1.a., 1.b., 1.c., 1.d., 1.e., 1.f., 1.g., 1.h., 1.i.), and will not plan to offer in Minnesota in the next 12 months unless demand were to change the offering status.

2. Public Health Transactions	Currently Offered	Plan to Offer in next 12 months
2.a. Electronic reporting of immunizations to MN Immunizations Information Connection (MIIC)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
2.b. Electronic submission of reportable lab results to MN Electronic Disease Surveillance System (MEDSS)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
2.c. Electronic submission of cancer cases to the MN Cancer Surveillance System	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
2.d. Other Registry transmissions, specify:	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
2.e. MDH Public Health Laboratory	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

CyncHealth is NOT currently supporting public health transactions to Minnesota State agencies (i.e., NO to 2.a, 2.b., 2.c., 2.e.). CyncHealth does support Public Health Transactions for the State of Nebraska through the Nebraska HIE and State of Iowa through the Iowa HIE.

Appendix A.3: Board of Directors

Justin	Birge	University of Nebraska Medical Center	986605 Nebraska Medical Cntr	Omaha	NE
Jaime	Bland	CyncHealth	11412 Centennial Rd	La Vista	NE
Mike	Cassling	Confluence Health	13808 F Street	Omaha	NE
Stephanie	Daubert	Nebraska Medicine	4350 Dewey Ave.	Omaha	NE
Stephen	Dolter	Children's Hospital and Medical Center	8200 Dodge Street	Omaha	NE
Matt	Edwards	Blue Cross and Blue Shield of Kansas City	2301 Main Street	KC	MO
Marty	Fattig	Nemaha County Hospital	2022 13th Street	Auburn	NE
Shari	Flowers	Nebraska Methodist Health System	825 S 169th St.	Omaha	NE
Jeff	Francis	Nebraska Methodist Health System	825 S 169th St.	Omaha	NE
Emily	Johnson	Sidney Regional Medical Center	1000 Pole Crk Xing	Sidney	IA
Raju	Kakarlapudi	Lincoln Lancaster County Health Dept	3131 O St.	Lincoln	NE
Ali	Khan	University of Nebraska Medical Center	984355 Nebraska Medical Cntr	Omaha	NE
Christopher	Maloney	Children's Hospital and Medical Center	8200 Dodge Street	Omaha	NE
Kristie	Stricklin	Boone County Health System	723 W Fairview St	Albion	NE
Chad	Werner	Blue Cross Blue Shield of Nebraska	1919 Aksarben Dr	Omaha	NE
Michael	White	Valleywise Health	2901 E Camelback Road	Phoenix	AZ
Jeanette	Wojtalewicz	CHI Health	12809 W. Dodge Road	Omaha	NE

Appendix A.2: Certificate of Good Standing



Certificate of Good Standing - Nonprofi

*Also included as "Appendix A"*

Appendix A.6: Conflict of Interest Policy



Excerpt from  
Employee Handboo

---

*Also included as “Appendix B”*

Appendix A.7: Audit



CyncHealth\_22  
NonGas FS\_Final.pdf

---

*Also included as separate attachment “Audit”*

Appendix A.8: Insurance



Certificate.pdf

---

*Also included as “Appendix C”*

Appendix B.3: Data Sharing Participation Agreement-Minnesota



MN PA.pdf

---

*Also included as “Appendix D”*

Appendix C.2: Privacy Policies



CyncHealth Privacy  
Policies \_ Final Rev 11

---

*Also included as “Appendix E”*



MINNESOTA  
PRIVACY POLICIES.pdf

---

*Also included as “Appendix F”*

## Appendix C.2: Security Policies



HITRUST Policies &  
Procedures.pdf

---

*Also included as separate attachment “Policies and Procedures”*

### **Attachment C: CyncHealth HIO Application Discussion**

#### **Minnesota Health Records Act (understanding and nuances of law)**

#### **4. Provide more detail on how the Minnesota-specific policies will be implemented, verified and monitored.**

The tools used internal to implement, verify and monitor legal requirements include: policies and procedures with regular review requirements, business owners for the technical implementation and monitoring, and education management system for training all applicable staff. We also have a compliance and cyber security committee that meets regularly and assists with escalated issues and HITRUST certification that we maintain.

For a new policy, CyncHealth uses the following processes:

1. Business owner receives approval from leadership for policy;
2. Business owner drafts policy for review by leadership and appropriate committees;
3. Legal team will review policy draft for statutory and regulatory compliance;
4. Committees and Board review as necessary. Some include our Data Governance Committee, Compliance and Cybersecurity Committee, Change Advisory Board, and our Board of Directors for any CyncHealth Entity;
5. Business owner revises and provides iterative documents for review as necessary;
6. Upon final approval of a policy the approved policy is saved and tracked in a central document repository;

7. Business owner is responsible for creating any training necessary and assigning the training to applicable personnel, after approval by leadership and Human resources;
8. Training is provided and tracked through our learning management system; and
9. Business owner reviews policy on a regular cadence (most often annually) as required.

**10. Describe how Minnesota requirements referenced in CyncHealth governance policies will be implemented and monitored for compliance?**

**Additional information requested: Provide a process for both internal and practices with participants. (Be sure to include psychotherapy note process – HIPAA, Minnesota's Health Records Act, and Psychotherapy Notes - October 2014 ([state.mn.us](http://state.mn.us)))**

The tools used to implement, verify and monitor requirements include: policies and procedures with regular review requirements, business owner monitoring of the technical implementation and learning management system for training all applicable staff. We also have a compliance and cyber security committee that meets regularly and adjudicates as needed escalated issues and supports our HITRUST certification.

If a new policy is needed to support a CyncHealth business or technical activity, the process identified above is used to create the policy.

Any auditing or monitoring of external parties (e.g., external audits of Minnesota providers to ensure they are adhering to consent requirements) would be documented in an internal policy and monitored and tracked by the business owner of that policy. Consistent with our audit practices and policies regular audits will occur as well as ad hoc reviews. Our Participation Agreements state that any Participant found to be in violation of our Participation Agreement or applicable law may be revoked or restricted from accessing or using the platform.

Regarding Information Security, CyncHealth has undergone several third-party assessments and successfully obtained a HITRUST(r2) certification, which also requires ongoing reviews to maintain certification. HITRUST is based upon nationally and internationally accepted security and privacy-related regulations, standards, and frameworks—including ISO, NIST, PCI, HIPAA, and GDPR—to ensure a comprehensive set of security and privacy controls. In addition, CyncHealth underwent a SOC 2 Type II certification.

**11. Describe how the “conspicuous check box” requirement for Opt-Out of an RLS or patient information service will be implemented for the CyncHealth longitudinal record.**

As noted in Minnesota 2023 Statutes, section 144.293 “Release or Disclosure of Health Records”, CyncHealth will only include patient information in the HIE after a patient, or authorized representative, provides a signed and dated consent for participation through a participating facility, including consent to participate in the Record Locator Service. The “Conspicuous Check Box” will be included in the consent form provided to patients by the participating facility and will clearly indicate the option for a patient to exclude information from the Record Locator Service by initialing the box and signing and dating the consent form. If the patient were to revoke consent, CyncHealth would follow the CyncHealth “Opt Out Policy” and “Opt Out Procedure” provided in this document.

Our technology providers and privacy program will maintain, and can produce, an audit log of providers accessing the service for a specific patient and the date information was accessed. Consistent with our privacy practices, CyncHealth conducts random and scheduled audits and also provides access logs as outlined in the Participation Agreement to participating facilities. Any misuse or abuse of the HIO could result in termination of the Participation Agreement for a facility or access to a provider.

**16. Describe how patient opt-out requests are accurately captured, tracked, and implemented.**

Minnesota residents must initially “opt in” to the CyncHealth HIE to have information available to query or access by a provider. Participating facilities would be responsible for offering the ability to “opt in” to the network and provide the requisite patient consent form (signed and dated) to CyncHealth. In the event a patient has formerly choose to “opt in” but decides to now “opt out” of the CyncHealth HIE, the following processes are followed (and detailed in the “Opt Out Procedure” and “Opt Out Policy”).

If a request is made by patient by phone, webform or postal service, the following procedures are followed:



Phone:

Patient would be asked to validate 6 out of the 7 pieces of personal information from the list below: (\* required)

- First Name \*
- Last Name \*
- Middle initial \*
- Date of Birth \*
- Address
- Phone number
- Facilities visited

Webform:

Patient may access the form via the CyncHealth public webpage at Opt In/Out (teamdynamix.com). CyncHealth will validate that the patient is in the HIE and call them at the number provided on the webform. During the call, CyncHealth will follow the phone validation process. If no one answers, we will leave the following message if possible “This is 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.” CyncHealth will not leave any identifiable information from the request. CyncHealth will make 3 calls but the request will not be processed if we do not receive a call back.

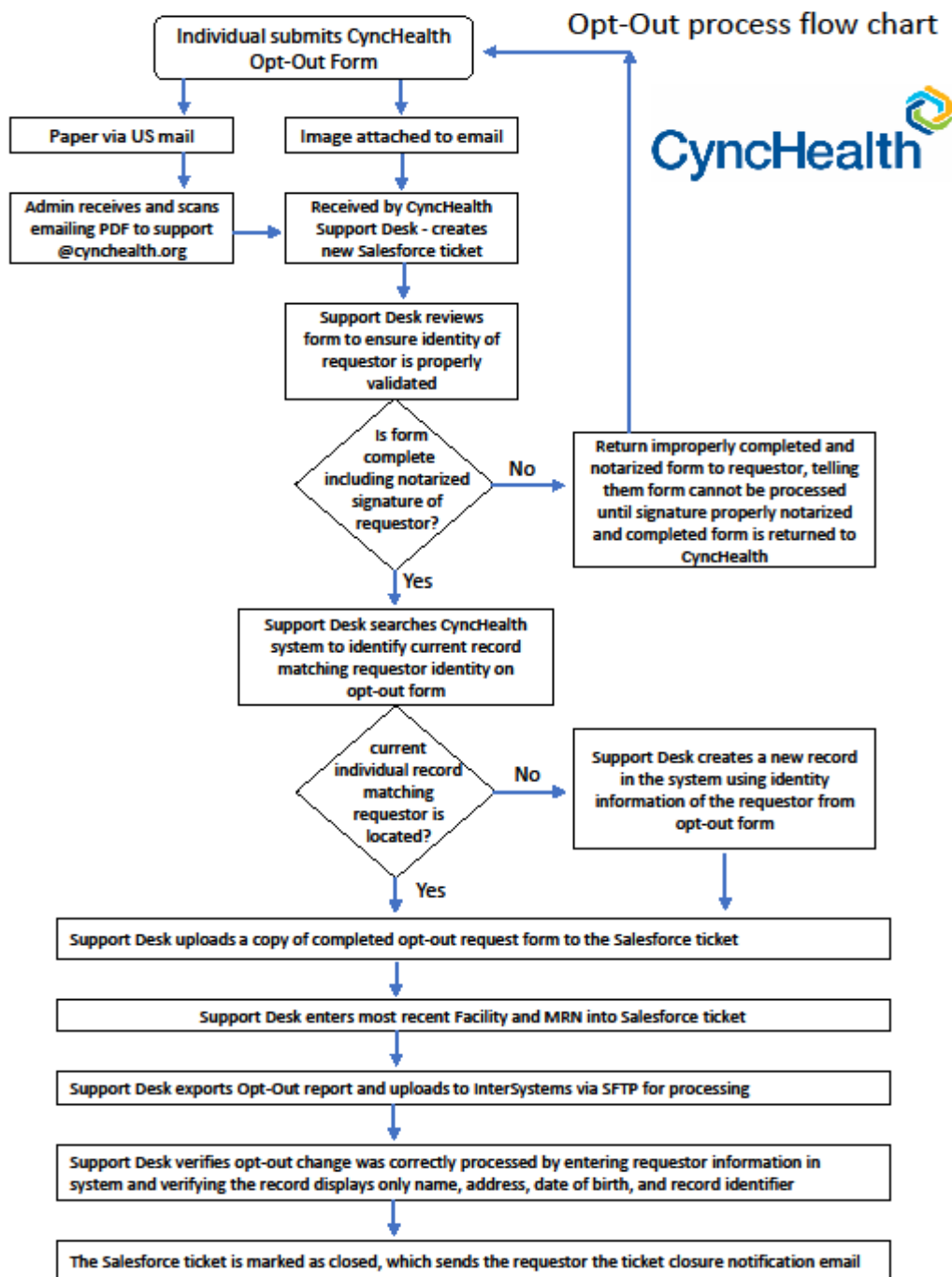
Postal Mail

CyncHealth will use the webform process identified above.

Regardless of contact method to CyncHealth, after the appropriate verification is received, CyncHealth will access the patient record in the HIE and set the MPIID to “opt out” using the “Opt Out Procedure”. CyncHealth will verify within the Record Locator Service and Clinical Viewer that the request was properly processed. (see workflow below)

CyncHealth will confirm with the participant that no facility will withhold coverage or care from an individual on the basis of that individual's choice not to have information viewable in the HIE. 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.

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.



**18. When opt-out occurs, what will show during a query (e.g., message returned is “no information found” versus “patient has opted out”)? Language on page 112 “*Opt-Out: A request to restrict the sharing of a patient’s health information that is viewable through the clinical viewer within the platform.*”**

**Additional information requested: Please refer to the MHRA Guidance for HIOs\_5.31.17.pdf (attached to email) for adjustments that may be required for the message response for a patient who has opted-out.**

When a provider queries a patient who has opted out of the HIE, the resulting query will show “null return”. This is similar to the opt out result for Nebraska patients and similar to other state HIEs. No accompanying demographic or other patient information will be presented during a query for patient’s who opt out.

**6. Provide detail on the CyncHealth privacy program, including a description and workflow diagram of the opt-out process, tracking methods to ensure that patient consent preferences are captured accurately (e.g., describe mechanisms to capture a patient consent flag), and detailed information outlining the auditing processes that are used (e.g., proactive, reactive, audit trails, etc.).**

CyncHealth uses the “Opt Out Policy” and “Opt Out Procedures” included above and the workflow above. Currently, we use a reactive process where a facility can make a written request to the CyncHealth Privacy Officer for an access report of one of its Authorized Users or a patient record during a specific period. CyncHealth would review the request and securely deliver the report to the requestor so the participant can validate that the records accessed were in compliance with HIPAA and the terms of our Participant Agreement. Audit trails can indicate the name of the Authorized User and the date(s) the patient record was accessed by the User. If a patient were to make a written request for a list of entities that have accessed or contributed information to their health record, the CyncHealth Privacy Officer would review the request and if the patient has a record and is not currently opted-out, CyncHealth would validate the identity using the process identified above and provide the patient with the names of any entities that have provided information or assessed their record covering the period in question. The CyncHealth Privacy Officer will advise the patient to approach the entity directly if they have any questions or concerns and offer to coordinate the initial contact. CyncHealth has received less

than 5 patient requests annually. If a participant operates an internal compliance program, CyncHealth also offers to provide an access report covering all of its Authorized Users at no cost every 6 months. We receive this type of request from 3-4 participants annually on average. To initiate this type of request the participant would complete and sign and submit a written request. CyncHealth would validate the information on the completed request form and obtain and securely deliver the report electronically.

CyncHealth has licensed a third-party software product to set up a more proactive HIPAA monitoring program as a value add to support its Participant's compliance efforts. We are in the process of implementing the software. The software is tailored to the healthcare industry and employs artificial intelligence to identify risk characteristics (neighbors, frequency or VIP record access, etc.). Weekly, the software would flag cases that are scored with the highest risk and CyncHealth would identify a relatively small number of those cases to investigate and resolve each week.

**7. Considering that states have different laws relating to health data privacy, describe how CyncHealth manages these requirements for residents of different states?**

CyncHealth currently successfully operates as an HIE in three states with different expectations for service and regulatory requirements. Our organization makes every attempt to standardize processes as required by federal laws or national certifying bodies or best practices. In cases where a state may have unique requirements or expectations, CyncHealth develops state specific policies, such as the "Minnesota Privacy Practices" or "Opt Out Policy". The state specific policies are created as outlined in the policy workflow above, approved by executive leadership and applicable Boards and Committees, and monitored by appropriate business owners at CyncHealth. Our legal team is sufficiently staffed, and our Compliance Officer is responsible for annually monitoring requirements and regulatory changes for the states we operate within as a certified HIO. Staff is empowered to identify, escalate, and operationalize necessary changes to ensure state specific compliance with all applicable laws.

**8. To ensure that CyncHealth is complying with the Minnesota Health Records Act, describe how a query for a Minnesota patient by a non-Minnesota provider is managed. Additional information requested: If not included with the “... process flow for both internal and practices with participant” requested above, include a process flow or mechanisms to capture a patient consent flag or other identification.**

CyncHealth maintains separate technical environments for each of our state HIEs. As allowed by federal and state laws, a Covered Entity with a permissible need may enter into a Data Sharing Participation Agreement for access to the state specific HIE. For example, a Nebraska hospital as a Covered Entity can enter into a Participation Agreement for the Nebraska HIE which covers Nebraska facilities. In Minnesota, the technical environment would allow Minnesota covered entities and their providers or business associates to enter into a Minnesota Data Sharing Participation Agreement for access to the Minnesota HIE. However, a Nebraska provider under a Nebraska Data Sharing Participation Agreement would be unable to access the Minnesota HIE clinical viewer to query a patient. Providers accessing the Minnesota HIE would need to be authorized to access the HIE by the covered entity with the Minnesota Data Sharing Participation Agreement.

### **Healthcare Payor Access**

**18. Describe how the following difference/requirement will be implemented by CyncHealth.**

**Health care payors in Minnesota are not allowed to access an HIO’s record locator service or patient information service. The current Data Sharing Agreement includes the following “... 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...”**

CyncHealth has updated the Minnesota “Data Sharing Participation Agreement” to reflect the above. Payors will not have access to information via a query or Record Locator Service and may only be provided data based on documented eligibility and pushed a secure file.

### **Interstate exchange**

**2. Clarify what type of exchange occurs at state borders. MDH thinks this may be exchange facilitated through the eHealth Exchange but please confirm.**

CyncHealth participates in ehealth exchange and does support data sharing across borders in this manner.

**9. How will query for Minnesota patient presenting for care in Iowa or Nebraska be managed (e.g., how will this be operationalized between states)?**

CyncHealth maintains separate technical platforms and data repositories for each state (e.g., Nebraska, Iowa). eHealth exchange currently facilitates exchange between Nebraska and Iowa and CyncHealth would use this process for Minnesota participants as well; however, other mechanisms could be used if needed dependent on the situation.

### **Social Determinants of Health/ Referrals to Community-Based Organizations**

**1. Elaborate on why HIE services are offered in only two states but the SDOH platform is offered in ten?**

CyncHealth leveraged federal Support Act funding to develop a network of community-based organizations (CBOs) using UniteUs as the technical partner. The funding supported the growth and expansion of a coordinated social care referral platform, separate from the state specific HIE. Since CBOs are not HIPAA Covered Entities, a distinct platform was necessary. CyncHealth's funding for the HIE in Nebraska and Iowa uses respective state and federal funds specific to operations for that state, under formerly HITECH and now via Medicaid Enterprise Systems Advanced Planning Documents (MES-APD).

### Query process

**3. Provide a detailed description of the query HIE service and plans for use in Minnesota. Include a picture of how technical vendor record locator service or patient information service will work.**

Our organization uses secure, certified vendors to support components of the HIE. The clinician portal offers the opportunity for a provider to interact with information within the HIE using a query process and known patient information. If a patient has opted out the provider will receive a “null result”.

CyncHealth uses an EMPI, which uses internal probabilistic algorithms and/or external matching modules to compare and match records in real-time. This creates an index of curated patient data and assigns an enterprise identifier to facilitate data exchange. To search for a patient in the platform, the provider enters the first and last name into the search box. Persons with similar names will return in the search. A numeric value to the right of the searched individual indicates the weight of the probability of the data returning in the search matching. The higher the value, the closer the likelihood of the match to your search criteria. Additionally, entering a date of birth or Medical Record Number (MRN) in addition to the first and last name is helpful in case of situations where more than one person has the same or similar first and last name and increases the probabilistic match of the desired patient.

### Funding/Sustainability

**11. Describe what is meant by “operational AND sustainable”. Would CyncHealth wait for sustainability in Minnesota before Minnesota representatives are added to a board? Or would a few Minnesota representatives be added as soon as there were Minnesota participants?**

CyncHealth has current participants with a Minnesota presence (e.g., Avera) and they are currently included on CyncHealth enterprise boards. CyncHealth is not likely to establish a Minnesota-specific board until there is more participation by Minnesota providers, and provider participation fees can support the operations.



**12. Describe what is meant by state participation fees. Does this refer to potential fees paid by the State of Minnesota or does this refer to fees paid by participating Minnesota organizations? The State of Minnesota does not have grant programs or other funding to pay participation fees at this time.**

CyncHealth participation fees in Minnesota will be paid by Minnesota providers participating in the Minnesota HIE, not the state.

### **Consumer Input**

**14. Since there is no longer a Patient and Family Engagement Committee, how are participating covered entities who have their own Patient Advisory Committees asked to represent that perspective on the standing committees (e.g., Data Governance Committee)?**

The CyncHealth Patient and Family Engagement Committee was sunsetted due to challenges maintaining a consumer perspective for a platform designed to engage and support providers not direct to consumers. CyncHealth works to capture the patient perspective by soliciting feedback from providers and hospitals with existing patient committees, through formal surveys, community events, and participant discussions.

### **Audits**

**17. Describe the frequency and scope of audits in the past two years (scheduled and random or participant requested)?**

Scheduled audits are completed annually by CyncHealth. Participants are offered the opportunity to receive access reports as a part of this auditing procedure, if requested in writing. CyncHealth puts onus on the participant to comply with the terms of the Participation Agreement and all federal and state guidelines. CyncHealth offers access to review authorized users/access every six months and assists with any investigations. As part of CyncHealth security processes and certifications we also have regularly scheduled audits conducted on systems by an independent third party.

**Others that can be answered via email**

**13. There was nothing in Attachment E; is the request for a Minnesota Certificate of Good Standing in process?**

The Minnesota Certificate of Good Standing is complete and documentation provided above.



**15. Describe current certification status of technical vendors. Indicate most recent information on certification status (most recent certification date and edition) with the Office of the National Coordinator for Health Information Technology (ONC) <https://chpl.healthit.gov/#/search>**

CyncHealth uses InterSystems as the technical partner.

InterSystems (ed. 2022.1)

<https://chpl.healthit.gov/#/listing/11076>

### Listing Information

<b>CHPL PRODUCT NUMBER:</b> 15.04.04.2988.Heal.21.07.0.221215	<b>ONC-ACB CERTIFICATION ID:</b> 15.04.04.2988.Heal.21.07.0.221215
<b>CERTIFICATION DATE:</b> Dec 15, 2022	<b>VERSION:</b> 2021.2
<b>CERTIFICATION EDITION:</b> 2015 Cures Update	<b>CERTIFICATION STATUS:</b> Active 
<b>ONC-AUTHORIZED CERTIFICATION BODY:</b> Drummond Group	<b>ONC-AUTHORIZED TESTING LABORATORY:</b> Drummond Group
<b>MANDATORY DISCLOSURES:</b> <a href="https://www.intersystems.com/products/healthcare-standards-certifications/#meaningful-use">https://www.intersystems.com/products/healthcare-standards-certifications/#meaningful-use</a> 	

### Developer

<b>DEVELOPER:</b> <a href="https://www.intersystems.com">InterSystems Corp.</a>	<b>DEVELOPER WEBSITE:</b> <a href="https://www.intersystems.com/HealthShare">https://www.intersystems.com/HealthShare</a> 
<b>SELF-DEVELOPER:</b> No	<b>Address:</b> 1 Memorial Drive Cambridge, MA 02142, USA
<b>Contact</b> Worldwide Response Center 617-621-0700 <a href="mailto:support@intersystems.com">support@intersystems.com</a>	

***MDH Legal Counsel Recommended revisions to consider (not required)***

**CYNCHALTH DATA SHARING PARTICIPATION AGREEMENT- MINNESOTA**

**21. MDH recommends adding a definition of Limited Data Set (3. Access to System, pg 26 of supplemental materials).**

This is included in the revised Minnesota “Data Sharing Participation Agreement” provided.

**22. Revise Clause 4.3 A to reflect specific state or Minnesota law rather than the authorization granted under HIPAA (page 32 of supplemental materials).**

This was updated and reflected in the revised “Minnesota Data Sharing Participation Agreement” provided.

**23. Revise/Remove 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... and 9.5 Funding Availability “**

This was updated as requested, and new language is included in the revised “Minnesota Data Sharing Participation Agreement”.

**Appendix A**

**Office of the Minnesota Secretary of State  
Certificate of Good Standing**

I, Steve Simon, Secretary of State of Minnesota, do certify that: The business entity listed below was filed pursuant to the Minnesota Chapter listed below with the Office of the Secretary of State on the date listed below and that this business entity is registered to do business and is in good standing at the time this certificate is issued.

Name: Nebraska Health Information Initiative, Inc.  
Date Filed: 01/08/2024  
File Number: 1443698300023  
Minnesota Statutes, Chapter: 303  
Home Jurisdiction: Nebraska

This certificate has been issued on: 01/10/2024



*Steve Simon*

Steve Simon  
Secretary of State  
State of Minnesota

**Appendix B**

## Excerpt from Employee Handbook

### 3.5 Conflicts of Interest/Outside Employment

CyncHealth employees are expected to devote their full business time and energy to performance of their duties for CyncHealth and should avoid any situation or activity that either conflicts with or creates the appearance of a conflict with the employee's responsibilities, or is otherwise at odds with the legitimate business interests of the CyncHealth. Business decisions must be made objectively, with CyncHealth's best interests in mind, and without regard to personal gain.

Employees must inform their supervisor in writing and receive written approval before engaging in any outside activities that pose the potential for conflict of interest, including, but not limited to:

- Any outside business activity that competes with the CyncHealth's current business
- Any outside business activity that represents a logical extension of the CyncHealth's current business or a business opportunity that CyncHealth would potentially pursue and within any potential line of business for CyncHealth
- Employment outside of CyncHealth which requires or allows for use of CyncHealth technology such as the HIE or PDMP
- Any time-consuming activity that detracts from one's ability to devote their full business time and energy to the Company's business (e.g., Employment outside of CyncHealth which might impact availability for a regularly scheduled shift)
- Employment within the CyncHealth enterprise in addition to your primary employment
- Any situation which may compromise one's judgment or cause one to show favoritism to a competitor, supplier, customer, or others
- The acceptance of gifts, gratuities, or favors from individuals or organizations with which CyncHealth conducts business or that are seeking association with CyncHealth or the extension of such gratuities or favors, which might reasonably be interpreted as an attempt to influence the recipients in the conduct of their duties



- The use of information CyncHealth considers privileged or confidential, for non CyncHealth purposes
- Using the name of CyncHealth for monetary profit or acting as a private person in a way that could create the impression you are speaking for CyncHealth;

Failing to report a potential conflict of interest immediately and receive proper supervisory approval or continuing an activity if your supervisor has disapproved it, is grounds for disciplinary action, up to and including termination of employment.

CyncHealth does not tell its employees how to spend time outside regular hours of employment. However, CyncHealth expects employees to not let any "moonlighting" activity, work, or hobby affect attendance, efficiency, or on-the-job performance. There should be no problem if an employee accepts outside employment as long as:

- The outside work or activity does not in any way lessen the employee's efficiency; and
- The outside work or activity does not present a conflict of interest, as discussed above.

All employees will be judged by the same performance standards and will be subject to CyncHealth's scheduling demands, regardless of any existing outside work requirements. The CEO must approve any exceptions to this policy in writing. If CyncHealth determines that an employee's outside work interferes with performance or the ability to meet the requirements of

CyncHealth as they are modified from time to time, the employee may be asked to terminate the outside employment if he or she wishes to remain employed with CyncHealth.

Nothing in this policy, whether by language or application, is intended to infringe upon any individual's right to engage in protected, concerted activity as defined by the National Labor Relations Act or any other employee legal rights.

**Appendix C**



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)  
12/15/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> HUB International Great Plains, LLC 11516 Miracle Hills Drive Suite 100 Omaha NE 68154	<b>CONTACT NAME:</b> Nicole Edmundson <b>PHONE (A/C, No, Ext):</b> 402.954.5531 <b>FAX (A/C, No):</b> 531.242.4411 <b>E-MAIL ADDRESS:</b> nicole.edmundson@hubinternational.com
	<b>INSURER(S) AFFORDING COVERAGE</b>
<b>INSURED</b> Nebraska Health Information Initiative, Inc. DBA CyncHealth PO Box 27842 Omaha NE 68127	<b>INSURER A:</b> Sentinel Insurance Company, Ltd. NAIC # 11000
	<b>INSURER B:</b> Hartford Insurance Group 914
	<b>INSURER C:</b> Hiscox Insurance Company 10200
	<b>INSURER D:</b> Crum & Forster Specialty Insurance Company 44520
	<b>INSURER E:</b> Houston Casualty Company 42374
<b>INSURER F:</b>	

**COVERAGES**      **CERTIFICATE NUMBER:** 1459187813      **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GENL AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input checked="" type="checkbox"/> LOC <input type="checkbox"/> OTHER			91SBAZI3000	8/1/2023	8/1/2024	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000 \$
A	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY			91SBAZI3000	8/1/2023	8/1/2024	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input checked="" type="checkbox"/> RETENTION \$ 40,000			91SBAZI3000	8/1/2023	8/1/2024	EACH OCCURRENCE \$ 5,000,000 AGGREGATE \$ 5,000,000 \$
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NE) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A	91WECBN088	8/1/2023	8/1/2024	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER E.L. EACH ACCIDENT \$ 500,000 E.L. DISEASE - EA EMPLOYEE \$ 500,000 E.L. DISEASE - POLICY LIMIT \$ 500,000
C D E	Crime Tech E&O/Cyber Liability Excess Cyber Liability			UC2490803523 TEO301999602 H23CX82074401	8/1/2023 8/1/2023 8/1/2023	8/1/2024 8/1/2024 8/1/2024	Crime Tech E&O/Cyber Excess Cyber \$1M \$5M Each Claim/Agg \$5M Each Claim/Agg

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)  
Named insured on Workers' Compensation policy is CyncHealth Advisors, Inc.

<b>CERTIFICATE HOLDER</b>  Proof of Insurance Only	<b>CANCELLATION</b> SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.
	AUTHORIZED REPRESENTATIVE 

© 1988-2015 ACORD CORPORATION. All rights reserved.

**Appendix D**

## CyncHealth Minnesota Participation Agreement

### 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, 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.

“Limited Data Set” means a compilation including PHI from which certain direct identifiers have been removed, as set forth in 45 C.F.R. § 164.514.

“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 and only as allowed under Minnesota Health Records Act:

(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 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.
- 9.5 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 no 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 CYNCHHEALTH, AND PARTICIPANT'S EXCLUSIVE REMEDY AGAINST CYNCHHEALTH, 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 CYNCEALTH**

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:

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
- Training session for each User that will be offered multiple times to reduce disruption
- 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 164.514l;
- (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 146 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 nonexclusive, 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.
- l. 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:

SIGNATURE AREA

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

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:

SIGNATURE AREA

**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:

Facility Name	Address
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.

**Appendix E**



# Privacy Policies

## Contents

INTRODUCTION	87
STATUS OF CYNCHHEALTH AND PARTICIPANTS.....	88
EFFECT OF LEGISLATION AND RULE CHANGES.....	89
Policy 100: Compliance with Law and Policy .....	91
Policy 200: Notice of Privacy Practices .....	94
Policy 300: Information Submission Policy.....	96
Policy 350: Opt-Out Policy.....	102
Policy 400: Access to and Use and Disclosure of Information .....	105
Policy 500: Minimum Necessary .....	114
Policy 600: Workforce, Agents, and Contractors .....	117
Policy 700: Individual Rights to Access to Health Information.....	120
Policy 800: No Information Blocking.....	123
Policy 900: Investigations; Incident Response System.....	125
Policy 1000: Information Security Policy .....	128
Policy 1100: Complaints About Uses and Disclosures of Confidential Information.....	133
Policy 1200: Breach Notification.....	136
Policy 1300: Insurance Requirements .....	139
Policy 1400: Privacy and Security Governance .....	141
Policy 1500: Privacy Officer.....	142
Policy 1600: Information Access Management.....	146

## CyncHealth Privacy Policies

### INTRODUCTION

The following policies apply to the access, use, and disclosure of Protected Health Information (PHI) or Personally Identifiable Information (PII) (collectively referred to as "Information") by CyncHealth staff and/or Participants through the CyncHealth Health Information Exchange (HIE) and other CyncHealth data analytics services being made available to Participants in CyncHealth (the HIE and other services are collectively referred to as the "System"). These policies will be reviewed and revised as needed based on the evolution of the System and any changing regulatory guidance. All capitalized terms will have the same meaning as defined below or as provided in the Data Sharing Participation Agreement ("Participation Agreement") or the Health Insurance Portability and Accountability Act ("HIPAA"), all as amended from time to time.

These CyncHealth Privacy Policies ("Policies"), taken together with privacy policies already deployed by Participants as covered entities under HIPAA or federal requirements, form a comprehensive array of administrative safeguards addressing the privacy of PHI or PII.

### Access and Use Limitation

PHI or PII should be accessed by one Participant from another Participant only pursuant to a mutual agreement that the Information will be used by the second Participant: (i) for the treatment, payment, or health care operations purposes of the Participant who disclosed it, (ii) the treatment, payment or health care operations purposes of the Participant who accessed it, or (iii) as specifically permitted by §164.512 of the Privacy Rule (Uses and Disclosures For Which Consent, an Authorization, or Opportunity to Agree or Object is Not Required), as permitted under these Policies and approved by the CyncHealth Compliance and Cybersecurity Committee ("Compliance and Cybersecurity Committee"). Information recipients may use and disclose PHI or PII obtained through the System only for purposes

and uses consistent with their permitted access and consistent with their obligations as covered entities under HIPAA or federal requirements. Certain exceptions, such as for law enforcement or public health, may warrant reuse of Information for other purposes. However, when Information obtained by a Participant through the System is used for purposes other than those for which the Information was originally obtained, the Participant using or disclosing the Information should first apply the rules applicable to it as a covered entity under HIPAA or Federal requirements and as a contracting Participant.

### **Security Safeguards and Controls**

Security safeguards are essential to privacy protection because they help prevent information loss, corruption, unauthorized use, modification, and disclosure. With increasing levels of cyber-crime, networked environments may be particularly susceptible without adequate security controls. Privacy and security safeguards should work together and be well coordinated for the protection of PHI or PII.

### **STATUS OF CYNCHHEALTH AND PARTICIPANTS**

Participants – those which provide data to the System and those which obtain and use data from the System – are either health care providers, health plans, health care clearinghouses, or other approved users (such as researchers) as outlined in Policy 100: Compliance with Law and Policy. All Participants are covered entities under HIPAA or Federal requirements or agree to be contractually bound to follow all HIPAA or Federal requirements rules and regulations as though they were a covered entity.

CyncHealth is a business associate ("BA") of the Participants. CyncHealth accepts and agrees to follow terms applicable to the privacy of PHI or PII by virtue of its business associate agreement with each Participant and these Policies.



## **EFFECT OF LEGISLATION AND RULE CHANGES**

CyncHealth and Participants need to remain flexible in approach in order to adapt to the uncertainty of state and federal legislation and regulations that will affect design, safeguards, rights and responsibilities over time. This shall include monitoring and implementing design components and safeguards mandated in the Health Information Technology for Economic and Clinical Health Act or “HITECH” as enacted in P.L 111-5 and regulations issued thereunder.

To permit Participants that disclose Information or whose Information is accessed to meet their obligation under HIPAA or federal requirements, and to address the need for safeguards, CyncHealth and Participants have placed the burden on the requesting Participant to access Information from the record of the disclosing Participant only:

1. When necessary and requested for the treatment, payment, or health care operations of the disclosing Participant (for example, to pay a claim submitted by the disclosing Participant or to render a consult requested by the disclosing Participant);
2. When necessary for the treatment, payment or "qualifying"<sup>1</sup> health care operations of the receiving Participant (for example, to obtain Information needed to submit a claim or to obtain Information needed to assess provider performance);
3. When the disclosure by the disclosing Participant is specifically permitted by §164.512(b) of the Privacy Rule and these Policies; and
4. In all cases, subject to the conditions and safeguards described in these Policies. In connection with disclosure for any payment or health care operations purposes, regardless of whether they are the payment or health care operations of the disclosing or receiving Participant, these conditions and safeguards include meeting the minimum necessary standard.

---

<sup>1</sup> Only a narrow subset of health care operations support disclosure for the health care operations uses of the recipient. This is discussed in detail in the Section "Special Rules for Disclosure for The Health Care Operations of the Recipient" under Policy 400 Access to and Use and Disclosure of Information.

5. As an additional safeguard, all Participants must be covered entities under HIPAA or Federal requirements or BAs of Participants under CyncHealth and therefore individually subject to regulation and penalties.
6. Participants may access PHI of others only for permitted purposes.

Special rules and conditions apply when disclosure is for the healthcare operations of the receiving Participant, and these are discussed in Policy 400.

## **Policy 100: Compliance with Law and Policy Scope and Applicability**

---

### **Laws**

Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of Protected Health Information (PHI) or Personally Identifiable Information (PII) and establishing certain individual privacy rights. Each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure compliance.

### **CyncHealth Policies**

Each Participant shall, at all times, comply with these Policies. These Policies may be changed and updated from time to time upon written notice to Participants in the manner described in the Participation Agreement. Any change to these Policies shall be effective when adopted by the CyncHealth Board of Directors, ordinarily following input by the CyncHealth Compliance and Cybersecurity Committee and the CyncHealth Data Governance Committee. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Policies.

### **Participant Policies**

Each Participant is responsible for ensuring that it has the appropriate and necessary internal policies for compliance with federal, state, and local statutes and regulations that are applicable to individuals who share or access Information (“Applicable Laws”) and these Policies.

### **Participant Criteria**

Each Participant shall itself be a HIPAA “covered entity” or a BA thereof and thus subject to both its individual legal duty as a regulated entity under HIPAA or HHS/Federal requirements

and its contractually assumed obligations under its Participation Agreement or Data Use Agreement. A BA of a Participant or a Qualified Entity (such as a Community-Based Organization that provides covered services) that is not a Covered Entity must be approved by the CyncHealth Data Governance Committee, CyncHealth Compliance & Cybersecurity Committee, and CyncHealth Board of Directors and agree to be contractually bound to follow all HIPAA or Federal requirements rules and regulations as though they were a covered entity before they can have access to the System in accordance with the Policies. As used in these Policies the term “Full Data-Sharing Participant” means a health care provider, entity, lab, pharmacy, health plan, or the like who:

1. enters into a data-sharing Participation Agreement;
2. shares all data pursuant to CyncHealth Policies according to the latest USCDI standard to the extent that the data is represented in the most recent version; and
3. pays an annual participation fee to sustain the connection and facilitate the bidirectional, longitudinal health record for the patient thereby promoting interoperability in accordance with federal regulations and guidance set forth by the ONC, CMS, and 21st Century Cures Act. Each Participant must agree to be a Full Data-Sharing Participant in order to become a data user, any exceptions would need to be approved by the CyncHealth Data Governance Committee.

### **Authorized User Criteria**

Authorized Users are individuals who have been granted access authority to the System as a result from a signed Participation Agreement. Therefore, each Authorized User must maintain a current relationship to a Participant in order to use the System. Authorized Users must therefore be: (i) Participants (for example, an individual physician) or workforce of a Participant, (ii) an individual BA or workforce of such BA, or (iii) an individual contractor or subcontractor of a BA or workforce of such contractor or subcontractor. Additionally, a Participant that is a covered health plan may also be an Authorized User in its role as a third-party administrator and BA for self-funded group health plans that are covered entities under HIPAA or Federal requirements but are not themselves Participants.

**Application to BAs and Contractors**

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

## Policy 200: Notice of Privacy Practices Scope and Applicability

### Policy

Each Participant shall develop and maintain a notice of privacy practices (the "Notice"). The Notice must describe the uses and disclosures of Protected Health Information (PHI) or Personally Identifiable Information (PII) contemplated through the Participant's participation in the System.

### Content

The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule<sup>2</sup> 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 PHI or PII through the

System. CyncHealth provides the following sample language for Participants who elect to amend their Notice:

*"We may make your protected health Information available electronically through an electronic health Information exchange to other health care providers that request your Information for their treatment, payment or health care operations purposes and to participating health plans that request your Information for their payment and health care operations. In all cases the requesting provider or health plan must have or have had a relationship with you. Participation in an electronic health information exchange also lets us see their Information about you for our treatment, payment and health care operations purposes. You have the right to opt out of sharing your protected health Information through CyncHealth. For more information, please visit [www.cynchealth.org](http://www.cynchealth.org)."*

---

<sup>2</sup> C.F.R. § 164.520(b). See 45 C.F.R. § 164.520(c)(2)(ii).

**Dissemination and Individual Awareness**

Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and, where applicable, acknowledgment of receipt by the individual, which policies and procedures shall comply with applicable laws and regulations.

**Participant Choice**

Participants may choose a more proactive Notice distribution or patient awareness process than provided herein and may include more detail in their Notice, so long as any expanded detail does not misstate the safeguards supporting the System.

**Policy 300: Information Submission Policy**

This policy applies to Participants and, where specifically stated, to Participants (or their designated Business Associates) that submit patient panels or member files to CyncHealth for attributed patients or members as required for the receipt of Participant Services as outlined in the Participation Agreement.

---

*Purpose*

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

*Policy*

Participants must provide access to data using content and manner standards that are supported by CyncHealth. This is necessary to ensure that the data supplied can be accessed, exchanged, and used by Participants for Permitted Uses, which may be changed according to the Participation Agreement.

Participants must complete testing and other onboarding activities prior to going live with connectivity to CyncHealth. These testing and onboarding activities are tailored to the type of data being provided and accessed and typically include a patient panel for those Participants who are health care plans. CyncHealth communicates these requirements during the onboarding process. Participants should notify CyncHealth of any changes prior to Participant's system changes or upgrades being made that would impact data sharing with CyncHealth. Information validation should be completed by comparing the data in CyncHealth's system to that in the Participant's source system. CyncHealth will provide guidance on testing, but it is the Participant's responsibility to execute a complete test plan in accordance with their own testing policies and procedures. Following the successful completion of participant testing, Participants must confirm that they are ready to go live.



### *Acceptable Data Formats*

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

1. HL7 V2
2. HL7 V3 (XML/CCD)
3. Claim and Claim Line Feed (CCLF) (Claims data only)
4. EDI/X12 (Claims information only)
5. Flat file formats (e.g., comma delimited)

Technology is constantly changing and improving. CyncHealth may accept and support other data formats in accordance with nationally recognized standards for HIE. Participants may consult, as needed, with their CyncHealth Account Manager to determine whether other content and manner standards may be accepted and supported by CyncHealth.

### *Information Integrity and Quality*

Each Participant shall use reasonable and appropriate efforts to assure that all Information it provides to CyncHealth is accurate, free from serious error, and reasonably complete. Each Participant shall cooperate with and assist CyncHealth in correcting any inaccuracies or errors in the Information it provides to CyncHealth.

### *Restriction of Uses and Disclosures*

If a Participant Covered Entity agrees to an individual's request for restrictions, as permitted under [45 CFR 164.522](#) of the HIPAA Privacy Rule or Federal Privacy Requirements, such Participant shall ensure that it complies with the restrictions. This shall include not making the individual's information available to the System, including advising the individual they have the right to opt-out of the System, if required by the restriction. Participants should advise individuals that opting out only affects access, use, and disclosure of their PHI or PII through the System and therefore does not prevent disclosure of their information from all systems

such as PDMP, or to their health care plans as set forth in the Opt-Out Impact Section in Policy 400 Opt-Out.

#### *Prohibited Data Submissions*

Some health information may be subject to special protection under federal, state, and/or local laws and regulations. Other health information may be deemed so sensitive that a Participant has made special provision to safeguard the information, even if not legally required to do so. Each Participant shall be responsible to identify what information is legally subject to special protection under applicable law and what information (if any) is subject to special protection under that Participant's policies, prior to disclosing any information through CyncHealth. Participants should not make Information requiring special protection available to the System.

#### **Information Not Furnished**

For System data to be useful, the Participant using it must know if it is complete or whether certain information would be withheld due to more stringent state and federal law or Participant policies. Applicable Law limits the circumstances under which certain types of data may be disclosed to CyncHealth and/or accessed and exchanged with other Participants. Because of these legal restrictions, and technical and operational complexities, it is not feasible for CyncHealth to support the exchange of certain types of data. Thus, Participants must NOT submit the following types of data to the HIE in any form:

1. Psychotherapy Notes (as defined by HIPAA);
2. Any other data that the Participant is not permitted by Applicable Law to disclose to CyncHealth and/or to make accessible to other Participants for Permitted Uses. For example, if a Participant chooses to grant an individual's request to restrict the use of the individual's data for HIPAA permitted Treatment, Payment, and Healthcare Operations purposes (other than HIPAA-Restricted Self-Pay information) or other Permitted Uses, Participant must not make this restricted data accessible through the

HIE because the technical and administrative processes necessary to honor the privacy restrictions are not currently available.

This is not intended to be an exhaustive list. Each Participant is responsible for complying with laws and regulations and its own policies regarding identifying and providing special treatment for information needing special protection.

### *Requirements for Protected Data Submissions*

1. **Part 2 Data Submissions.** Federal law gives greater privacy protections to 42 CFR Part 2 Information (“Part 2 Data”). CyncHealth must segregate Part 2 Information to comply with these more restrictive requirements and only redisclose according to patient consent. CyncHealth segregates all data from Participants who attest they are a Part 2 Participant or operate a Part 2 program from other data accessible through CyncHealth. CyncHealth segments Part 2 information for those Mixed Use Participants based on their attestation during the onboarding process. Before submitting any data to the HIE, Participants must notify their designated CyncHealth Account Manager in writing if they operate a Part 2 Program so CyncHealth can properly manage the data according to applicable workflows and consents required.
2. **HIPAA-Restricted Self-Pay information.** HIPAA gives individuals the right to ask their healthcare providers not to disclose protected health information (PHI) to health plans, where individuals have paid for healthcare services in full out-of-pocket and the PHI relates to those healthcare services. HIPAA requires healthcare providers to honor such requests. For Participants and CyncHealth to comply with such restrictions, the Participant must not make the HIPAA-Restricted Self-Pay information accessible through CyncHealth.
3. **Requirements for Patient Panel and Member File Submissions.** Some HIE Services (i.e., Patient Alerts and certain HIE reporting services) require Participants or their designated Business

Associates to supply CyncHealth with an up-to-date patient panel or member file for attributed Individuals (collectively, “Patient Panels”), which CyncHealth utilizes to route HIE data to Participant in accordance with the Permitted Use Policy. Such Participants must submit Patient Panels in accordance with the following requirements.

- A) All Participants must submit Patient Panels that comply with CyncHealth’s standard Patient Panel specifications, which are supplied during the HIE onboarding process. By including an Individual on Participant’s Patient Panel, the Participant represents that it has a current HIPAA-compliant Treatment, Payment, or Healthcare Operations relationship with the Individual. However, Health Plans may access certain Information of a terminated member for a limited time in compliance with the Participation Agreement.
- B) After the submission of an initial Patient Panel, all Participants must update and refresh such Patient Panels via submission of a delta file that indicates which Individuals should be added or deleted from Participant’s Patient Panel and follows the standard specification for delta file submissions provided by CyncHealth during implementation. If a Participant does not have the technical ability to update a Patient Panel via submission of a delta file, then such Participant must receive written approval from CyncHealth to submit updates to a Patient Panel via an alternative method.
- C) Health Plans: Health Plans must update their Patient Panels at least monthly or more often if requested by Participant and agreed upon by CyncHealth. If a Health Plan Participant fails to update their Patient Panel at least monthly, then CyncHealth has the right to discontinue the delivery of applicable data services until a delta file with updates is delivered and processed.
- D) Providers: In the event a Participant chooses to use a CyncHealth product that requires a Patient Panel, then the Participant is responsible for notifying CyncHealth of changes to their Patient Panel via the provision of a delta file or other mutually

agreeable alternative method. When Provider no longer has a HIPAA-compliant reason to receive data for an Individual, Provider must notify CyncHealth as soon as possible by providing an updated delta file but in no case any less frequently than annually.

## **Policy 350: Opt-Out Policy**

An Opt-Out is a request to restrict the sharing of a patient's health information that is viewable through the clinical viewer within the platform.

### *Opt-Outs*

All individuals will have the opportunity to opt out of participating in the health information exchange or to opt-in following their prior opt-out.. A request to opt out will be treated as a request for restrictions on use and disclosure of Protected Health Information (PHI) or Personally Identifiable Information (PII) within the health information exchange.

### *Request Process*

CyncHealth will provide opt-out information and downloadable PDF request form on a public website. An opt-out or opt-in request will be initiated and received in paper form In addition, CyncHealth may upon request send a paper opt-out or opt-in request form to the individual for the purposes of opt-out. Once a completed and notarized opt-out or opt-in is received and validated by CyncHealth, it will be processed within 30 calendar days.

### *Participant Communication*

Participants may access and download data sharing educational material on CyncHealth's 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 method for opting out or opting in will be available. CyncHealth will define the scope of an opt-out applied to the individual health information to include the advantages of sharing health information and the disadvantages of the r 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 staff to answer questions about data sharing via exchange networks to include CyncHealth.

CyncHealth will document opt-out/opt-in-processing procedures and train the support staff on the procedures including the process for identity verification of the individual signing the request form.

The Compliance and Cybersecurity 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 having their information viewable in the health information exchange, the effect is applied as follows:

1. an individual's clinical data would not be accessible by search or query by a Participant's Authorized User of the health information exchange application only; and
2. an individual's data will still flow into the HIE but will not be viewable except for name, address, and opt-out status;
3. An individual's decision to opt-out of participating in the health information exchange :may be changed at any time by the individual by providing a completed opt-in written request form to the support desk of the health information exchange;
4. does not prohibit use or disclosure of individually identifiable health information, which is required by law or authorized under the Public Health statute [Nebraska Statutes 81-601];
5. does not apply to all systems or applications operated by CyncHealth (i.e., public health applications such as PDMP, or eMPI);
6. does not prevent health plans from accessing the health information of its members as authorized under HIPAA including to fulfill coverage responsibilities, providing benefits under the plan, and providing reimbursement for the provision of healthcare; and

7. does not prohibit disclosure of health information if the disclosure is required by law.

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, via direct secure message or notifications required under the final interoperability rule [85 FR 25510].



## **Policy 400: Access to and Use and Disclosure of Information**

### **Compliance with Law**

Participants shall access, use, and disclose Protected Health Information (PHI) or Personally Identifiable Information (PII) through CyncHealth only in a manner consistent with all applicable federal, state, and local laws and regulations and not for any unlawful or discriminatory purpose.

### **Documentation and Reliance**

If applicable law requires that certain documentation exist or that other conditions be met prior to disclosing PHI or PII to CyncHealth for a particular purpose, the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions. Each access and use of PHI or PII by a Participant is a representation to every other Participant whose PHI or PII is being accessed and used that all prerequisites under state and federal law for such disclosure by the disclosing Participant have been met.

### **Purposes**

A Participant may request and use PHI or PII from other Participants through the System only:

1. to participate in treatment (in the case of providers), payment or health care operations of the disclosing Participant;
2. to conduct treatment (in the case of providers), payment and qualifying health care operations purposes of the requesting Participant; or
3. for those purposes specifically permitted by §164.512(b) and §164.512(i) of the Privacy Rule and approved by the Data Governance Committee, and then only to the extent necessary and permitted by applicable federal, state, and local laws and regulations and these policies, including any required conditions imposed by the Committee. A Participant may request and use PHI or PII through the System only if the Participant has or has had

or is about to have the requisite relationship to the individual whose PHI or PII is being accessed and used except for the subsequent Use and Disclosure Paragraph below.

### **Prohibitions**

Information may not be requested for fundraising, marketing or purposes related to fundraising or marketing without specific patient authorization. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request or access information through the System.

### **CyncHealth Permitted Uses**

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

1. As required by law, including if required by a subpoena that satisfies the requirements of Applicable Law;
2. As necessary to perform services under the Participation Agreement and to assist Participants (and Participants' Business Associates) in the Permitted Uses;
3. As directed in writing by the providers of the information;
4. To provide access to an individual in accordance with Applicable Law and the Patient Access Policy;
5. To provide access to a person or entity that has a HIPAA Authorization to access PHI and PII of the individual who is the subject of the HIPAA Authorization for the purposes given in the HIPAA Authorization ("Authorized Recipients"), such as Insurance Companies, if CyncHealth has the necessary technical and administrative processes in place to support Authorized Recipients access in accordance with Applicable Law and healthcare industry-standard security practices;

6. To conduct Healthcare Operations on behalf of Covered Entities;
7. To conduct Limited Public Health Activities;
8. To facilitate health information exchange through Trusted HIE Connections for any of the Permitted Uses set forth in this policy, including (but not limited to) Treatment, Payment, Healthcare Operations, and Limited Public Health Activities;
9. To create De-Identified information to be used and disclosed for purposes permitted by Applicable Law ); and
10. For CyncHealth's own management and administration (including but not limited to the operation of its master person index) or to carry out its legal responsibilities, including (but not limited to) audit, legal defense, and liability, record keeping, and similar obligations.

### **CyncHealth Policies**

Participant uses and disclosures of, and requests for, PHI or PII through the System shall comply with CyncHealth's policies on Minimum Necessary and Information Subject to Special Protection.

### **Subsequent Use and Disclosure**

A Participant that has accessed information through the System and merged the information into its own record shall treat the merged information as part of its own record and thereafter use and disclose the merged information only in a manner consistent with its own information privacy policies and laws and regulations applicable to its own record. A Participant shall not access PHI or PII through the System for the purpose of disclosing that information to third parties, other than for the Participant's treatment, payment, or qualifying healthcare operations purposes.

### **Secondary Use of CyncHealth Information**

CyncHealth management may, on behalf of a Participant or other entity, submit to the CyncHealth Data Governance Committee a written request to use CyncHealth data for secondary uses, such as for healthcare operations, for public health activities or for research, including reviews preparatory to research, subject to the following rules:

1. De-identified data. Participants or other approved entities may request deidentified data sets for healthcare operations, public health, and/or research purposes. The Participant or other entity shall specify the purpose for which the de-identified data will be used; will attest that it will not use the deidentified data for other purposes, transfer it to third parties for other purposes, re-identify the deidentified data, or sell or lease the data; and shall enter into a data use agreement with CyncHealth.
2. Limited data set. Participants or other approved entities may request a limited data set for public health or research purposes by entering into a data use agreement with CyncHealth. The Participant or other approved entity must have Institutional Review Board (IRB) approval to obtain a limited data set for research purposes.
3. The CyncHealth Data Governance Committee shall review and recommend approval/disapproval of each request and will obtain any other additional approvals prior to disclosure, such as the Nebraska Health Information Technology Board established in Neb. Rev. Stat. §81-6,128.

### **Disclosures to Law Enforcement**

As permitted by § 164.512(f) of the Privacy Rule, if a law enforcement official requests PHI from CyncHealth via a court order, subpoena, warrant, summons, or other similar document, CyncHealth shall provide such documentation without unreasonable delay to any applicable Participant who as a Covered Entity may provide the requested PHI as required by and in accordance with city, state, and federal law without first obtaining specific patient authorization:

1. to assist in the identification or location of a suspect, fugitive, material witness, or missing person;
2. regarding a patient who is or is suspected to be a victim of a crime;
3. to alert law enforcement of the death of the individual;
4. if CyncHealth believes the PHI requested constitutes evidence of criminal conduct that occurred on the premises of CyncHealth;
5. in emergency situations, to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime; and only if: A) the PHI sought is relevant and material to the law enforcement inquiry;  
  
B) the request is specific and limited in scope to the extent reasonably practicable;  
  
C) de-identified PHI could not be used; and  
  
D) the court order, subpoena, warrant, summons, or other similar document complies with Nebraska law which in some cases requires patient authorization to release.

If a CyncHealth employee is presented with a court order, subpoena, warrant, summons, or other similar document, the employee should immediately notify the CyncHealth Privacy Officer of the document who will evaluate the document and determine whether and how the request will be directed. No PHI should be disclosed in response to a court order, subpoena, warrant, summons, or other similar document prior to discussing the document with the Privacy Officer.

The Participant providing PHI in response to a court order, subpoena, warrant, summons, or other similar document is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided, the agency name and address (if known), the

date the PHI was provided, and a summary of the PHI provided for each patient whose PHI is reported or released.

Documentation of releases and disclosures that are made by CyncHealth in response to a court order, subpoena, warrant, summons, or other similar document shall be maintained by the Privacy Officer or his or her designee. All documentation relating to requests for a patient's PHI shall be maintained for a minimum of six (6) years.

### **Responding to Inquiries from National Security, Intelligence, and Protective Services Officials**

As permitted by § 164.512(k) of the Privacy Rule, if a federal official requests PHI from CyncHealth for intelligence, counterintelligence, and other national security activities, CyncHealth may provide the requested PHI as required by and in accordance with city, state, and federal law without first obtaining specific patient authorization. The CyncHealth employee receiving such request should immediately contact the CyncHealth Privacy Officer.

The CyncHealth Chief Information Security Officer providing PHI to authorized federal officials for national security and intelligence activities and protective services is responsible for documenting the name, title, and contact information of the individual to whom the PHI was provided, the agency name and address, the date the PHI was provided, and a summary of the PHI provided for each patient whose PHI is reported or released.

Documentation of releases and disclosures of patient's PHI that are made to authorized federal officials for national security and intelligence activities and protective services shall be maintained by the Privacy Officer or his or her designee and retained for a minimum of six (6) years.

### **Audit Logs**

Participants and CyncHealth shall develop an audit log capability to document which Participants posted and accessed the information about an individual through the System and when such information was posted and accessed. Upon request of a Participant to assist with their internal investigation related to a complaint, CyncHealth shall provide one-time reports as are necessary to determine and/or document user access including what information was accessed by a given user and when such information was accessed. At no cost no more than every six months, upon the written request of the Participant's Privacy Officer, to assist in Participants compliance program CyncHealth shall provide a report showing all of Participants Authorized User access in the System including what Information was accessed and when such information was accessed by each Authorized User.

### **Authentication**

Participants must adhere to the authentication procedures established by CyncHealth to verify each user's identity before they are granted access to CyncHealth systems.

### **Application to BAs and Contractors**

Participants shall apply these Policies to their BAs and to the contractors and subcontractors of their BAs as appropriate.

### **Special Rules for Disclosures for the Health Care Operations of the Recipient**

The authority for a covered entity to disclose protected health information to another covered entity for the other covered entity's health care operations is subject to the following 5 conditions:

1. The recipient must be a covered entity.
2. Only health care operations activities described in subsections (1) and (2) of the regulatory definition of health care operations will support the disclosure by the disclosing Participant or access by the receiving Participant. These activities represent

a narrow subset of the full list of health care operations. To draw attention to the limited nature of these health care operations, these Policies refer to them as "qualifying" health care operations. Per the Privacy Rule, they consist only of the following activities:

- A) "Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- B) 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."

No other health care operations activities of a requesting Participant will support access or disclosure. Thus, although a Participant could access or disclose protected health information of its own patients for a much broader array of its own health care operations activities, it may only access information from another Participant for "qualifying" health care operations.

- 3. The recipient must have or have had a relationship with the individual who is the subject of the information being disclosed. For example, if a health plan Participant requests PHI for the Plan's health care operations, access would be limited to individuals who then were or who had been covered enrollees of the health plan.



4. The information accessed or disclosed must pertain to the relationship. For example, if a health plan Participant requests PHI for the plan's health care operations, access would be limited to the period of the individual's enrollment in the health plan's plan.
5. The disclosure, and therefore the access, is subject to the minimum necessary rule.

In addition, a Participant desiring to utilize the protected health information of other Participants for its healthcare operations must first obtain approval of the CyncHealth Data Governance Committee as set forth below:

1. The Participant's "Use Case" must be included in the request to the CyncHealth Data Governance Committee for review, discussion, and approval. An approved Use Case will include the conditions and safeguards the Committee determines are necessary and reasonable to permit the proposed acquisition and use for qualifying health care operations. The approval will be by function, not requesting Participant, and other Participants may act on the authority of an approved Use Case.
2. A Participant that relies on a Use Case already approved by the CyncHealth Data Governance Committee, must notify the CyncHealth Data Governance Committee of its intent to access protected health information for its own qualifying health care operations and agree to meet the conditions of the approved Use Case.
3. All Participants acting in reliance on an approved Use Case must conform to all conditions in the approved Use Case.

CyncHealth will retain documentation of all Use Cases submitted for approval including any conditions and safeguards the Committee determines are necessary and reasonable to permit the proposed acquisition and use for qualifying healthcare operations.

## **Policy 500: Minimum Necessary**

### **Requests**

When requesting or accessing PHI or PII of other Participants for payment or qualifying health care operations purposes, each Participant shall request only the minimum amount of health information through the System as is necessary for the intended purpose of the request.

### **Disclosures**

A Participant is entitled to rely on the scope of a requesting Participant's request for information as being consistent with the requesting Participant's minimum necessary policy and needs.

### **Workforce, BAs, and Contractors**

Each Participant shall adopt and apply policies to limit access to the System to members of its workforce who qualify as Authorized Users and only to the extent needed by such Authorized Users to perform their job functions or duties for the Participant.

### **Entire Medical Record**

A Participant shall not use, disclose, or request an individual's entire medical record unless necessary and justified to accomplish the specific purpose of the use, disclosure, or request.

### **Application to Health Plans**

A Participant that is a health plan shall access and use PHI of another Participant only: (i) for "payment" purposes of the health plan or disclosing Participant as described in 42 C.F.R. § 164.501, or (ii) for qualifying "health care operations" purposes as described under Section 16 ("Special Rules for Disclosure for the Health Care Operations of the Recipient") of Policy 400.

Participants that are health plans shall initiate a search through the System for payment purposes only:

1. to obtain premiums or to determine or fulfill their responsibility for coverage and provision of benefits under the health plan;
2. to obtain or provide reimbursement for the provision of health care;
3. to determine eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
4. to risk adjust amounts due based on enrollee health status and demographic characteristics;
5. for 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;
6. to review health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and,
7. for utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services.

All Participants shall access and use only the minimum information necessary when accessing and using information for payment or qualifying health care operations purposes. A Participant that is a health plan shall not access protected health information related to a specific encounter and/or treatment of a patient if the patient has paid the health care provider directly out of pocket in full for such encounter and/or treatment.

**Application to Providers and Treatment Purposes**

While this minimum necessary policy is not required by HIPAA or Federal requirements for providers accessing, using, and disclosing protected health information for treatment purposes, they are encouraged to follow it when consistent with treatment needs.

**Application to BAs and Contractors**

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

## **Policy 600: Workforce, Agents, and Contractors Scope and Applicability**

### **CyncHealth Responsibility**

CyncHealth is responsible to establish and enforce policies designed to comply with its responsibilities as a BA under HIPAA or Federal requirements and to train and supervise its workforce to the extent applicable to their job responsibilities.

### **Participant Responsibility**

Each Participant is responsible to establish and enforce policies designed to comply with its responsibilities as a covered entity under HIPAA or Federal requirements and a Participant in the System, and to train and supervise its Authorized Users to the extent applicable to their job responsibilities.

### **Authorized Users**

All Authorized Users, whether members of a Participant's workforce or members of the workforce of a BA or contractor, shall execute an individual Authorized User agreement and acknowledge familiarity with and acceptance of the terms and conditions on which their access authority is granted. This shall include familiarity with applicable privacy and security policies of the Participant, BA, or contractor, as applicable. Participants shall determine to what extent members of their workforce, or the workforce of BAs and contractors, require additional training on account of the Participant's obligations under their participation agreement and these policies and arrange for and document such training. CyncHealth shall reserve authority in the Participation Agreement to suspend, limit or revoke access authority for any Authorized User or Participant for violation of Participant and/or CyncHealth privacy and security policies.

### **Access to System**

Each Participant shall allow access to the System only by those Authorized Users who have a legitimate and appropriate need to use the System and/or release or obtain information through the System. No workforce member, agent, or contractor shall have access to the System except as an Authorized User on behalf of a Participant and subject to the Participant's privacy and security policies and the terms of the individual's Authorized User agreement.

### **Access Audits**

All Participants are required to monitor and audit access to and use of their information technology systems in connection with the System and in accordance with their usual practices based on accepted healthcare industry standards and Applicable Law. In the event CyncHealth wishes to exercise its right to audit the Participant, the Participant will provide CyncHealth with monitoring and access records upon request. CyncHealth may review the usage of the Participant Authorized User's access to patient records and will Participant will enforce any confirmed misuse by an Authorized User in accordance with the terms of the Participation Agreement. It is ultimately the Participant's obligation to ensure the appropriate use of the CyncHealth System by the Participant and its Authorized Users.

### **Discipline for Non-Compliance**

Each Participant shall implement procedures to discipline and hold Authorized Users, Bas, and contractors accountable for following the Participant's policies and for ensuring that they do not use, disclose, or request PHI or PII except as permitted by these Policies. Such discipline measures may include, but not be limited to, verbal and written warnings, restriction of access, demotion, and termination, and may provide for retraining where appropriate.

### **Reporting of Non-Compliance**

Each Participant shall have a reporting procedure, and shall encourage all workforce members, BAs, and contractors to report any non-compliance with the Participant's policies or

the policies applicable to Authorized Users. Each Participant also shall establish a mechanism for individuals whose health information is included in the System to report any non-compliance with these Policies or concerns about improper disclosures of PHI or PII.

### **Enforcing BAAs and Contractor Agreements**

Each Participant shall require in any relationship with a BA, contractor, or other third party (which may include staff physicians) that will result in such third party becoming an Authorized User on behalf of the Participant, or that will result in members of the workforce of such third party becoming Authorized Users on behalf of the Participant, that:

1. such third party and any members of its workforce shall be subject to these Policies accessing, using, or disclosing information through the System;
2. that such third party and/or Authorized Users of its workforce may have their access suspended or terminated for violation of these Policies or other terms and conditions of the Authorized User agreement; and
3. that such third party may have its contract with the Participant terminated for violation of these Policies or for failure to enforce these policies among its workforce.

## **Policy 700: Individual Rights to Access to Health Information**

### **Individual Requests to Access Their Health Information**

HIPAA in 45 CFR § 1564.524, provides individuals the right of access to inspect and obtain a copy of their own health information unless an exception to the individual right of access applies. Because CyncHealth does not have a direct relationship with individuals whose health information is accessible through the HIE, CyncHealth must rely on its Participants to manage relationships and disclosures of patient information, including health information available in the CyncHealth System, to patients. Patients who contact CyncHealth requesting access to their healthcare Information will be referred to one or more of the Participants where they receive care. Due to legal, technical, and administrative limitations, the CyncHealth system does not currently support alternative means by which patients may access their health Information through the HIE, such as through an individual access portal or other automated means. Each Participant should have a formal process through which it permits individuals to view information about them that has been posted by the Participant to the System. CyncHealth shall work towards providing patients direct access to the information about them contained in the System. Until that time, CyncHealth will process such written requests in accordance with the Patient Requested Access Report process described below.

### **Accountability of Disclosures**

HIPAA in 45 CFR § 164.528 provides an individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested. Because CyncHealth is the Business Associate and has contractually agreed in compliance with Applicable Law to refer every request for an accounting of disclosures to the appropriate Participant who is the Covered Entity, CyncHealth will require any individual making an accounting of disclosures request to first submit the completed, signed and notarized Health Information Request Form available at [www.cynchealth.org](http://www.cynchealth.org). Upon receipt of a completed signed and notarized Information Request Form, CyncHealth will respond that there was no record match in the System, or in



the event of a record match, the response will list the applicable Participant(s) who CyncHealth has referred the completed and validated request and the Participant shall respond directly to the individual who made the request for accounting of disclosures in compliance with Applicable Law.

### **Patient Requested Access Report**

Upon receipt of a completed signed and notarized Information Request Form available at [www.cynchealth.org](http://www.cynchealth.org), CyncHealth will either provide an individual a response that there was no record match in the System or in the event of a record match, CyncHealth will provide the individual with a list of healthcare providers and the dates they accessed their health information through the System. The list will also include the names of healthcare providers who have contributed to the individual's own health record in the System. If after review of the list, the individual indicates a desire to request a copy of their own health information from such healthcare provider(s), CyncHealth will offer to obtain the proper contact staff and provide the contact information to the individual.

### **Individual Amendment Requests**

HIPAA gives individuals the right to request an amendment to their health information. CyncHealth has no authority or control over the accuracy or completeness of the information provided by Participants. CyncHealth will notify affected Participants if CyncHealth receives an amendment request directly from an individual (or an individual's personal representative). Participants are responsible for responding to individual amendment requests in the manner and within the timeframe required by Applicable Law. Only the Participant responsible for the record being amended may accept an amendment. If one Participant believes there is an error in the record of another Participant, it shall contact the responsible Participant.

A Participant shall notify CyncHealth when it has amended an individual's PHI or PII via a mechanism developed by CyncHealth.

**Application to BAs and Contractors**

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

## **Policy 800: No Information Blocking**

### **Application to BAs and Contractors**

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

### **Compliance with the Information Blocking Rule**

The 21<sup>st</sup> Century Cures Act (CURES) and its implementing regulation (the Information Blocking Rule see 45 C.F.R. Part 171 (IBR)) prohibits “information blocking,” which is a practice engaged in by a health care provider, health IT developer of certified health IT, health information network or health information exchange (an “Actor”), that interferes with the access, use or exchange of Electronic Health Information (“EHI”). CyncHealth and Participant Actors will fulfill requests for EHI as set forth in the IBR. Actors may be subject to penalties or disincentives if they violate the IBR by engaging in Information Blocking practices with the requisite level intent, and if the practice is not explicitly required by law or does not qualify for a regulatory exception set forth in the IBR (a “Safe Harbor”).

CyncHealth and Participant Actors may not engage in any practices that violate the IBR in connection with HIE services. This policy does not prevent CyncHealth or Participant Actors from engaging in practices that are explicitly required by law or that fall within a Safe Harbor.

CyncHealth and Participant Actors are each independently responsible for identifying, assessing, and determining whether its own practices implicate the prohibition on Information Blocking, are explicitly required by law or qualify for a Safe Harbor. The Participation Agreement and these Policies are designed to comply with the Content and Manner Exception by specifying the mutually agreed upon terms and conditions that govern the access, exchange, and use of information by Participants.

The IBR also expressly recognizes that Actors, like Health Information Exchanges, must impose restrictions on those who seek to access, exchange or use EHI because those restrictions promote a larger public purpose such as making certain that the privacy and security of EHI is protected and that only those who are authorized can actually access, exchange or use EHI.

### **Information Blocking Complaints**

CyncHealth and its Participant Actors will each document their reasons for not fulfilling a request for EHI to the best of their ability so that a record exists in the event that an information-blocking complaint is filed. Participants that reasonably believe CyncHealth or a Participant Actor is violating the IBR in connection with the HIE Services should promptly notify CyncHealth. Complaints may be submitted anonymously through the CyncHealth website [www.cynchealth.org](http://www.cynchealth.org).

CyncHealth may initiate an investigation into a complaint of IBR involving a Participant Actor and/or take any other appropriate action, depending on the facts and circumstances surrounding the complaint. The investigation of any complaint will be reported to the Compliance and Cybersecurity Committee to ensure communication, transparency, and oversight.

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

## **Policy 900: Investigations; Incident Response System Scope and Applicability**

### **Incident Response**

CyncHealth shall implement an incident response system in connection with known or suspected privacy breaches, whether reported by Participants or discovered by CyncHealth. The incident response system shall include the following features, each applicable as determined by the circumstances:

1. cooperation in any investigation conducted by the Participant or any direct investigation conducted by CyncHealth;
2. notification of other Participants or Authorized Users as needed to prevent further harm or to enlist cooperation in the investigation and/or mitigation of the breach;
3. cooperation in any mitigation steps initiated by the Participant or CyncHealth;
4. furnishing audit logs and other information helpful in the investigation;
5. developing and disseminating remediation plans to strengthen safeguards or hold Participants or Authorized Users accountable;
6. any other steps mutually agreed to as appropriate under the circumstances; and,
7. any other step required under the incident reporting and investigation system.

### **CyncHealth Cooperation**

CyncHealth shall cooperate with a Participant in any investigation of the Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self investigation by the Participant, when the investigation implicates

CyncHealth conduct, or the conduct of another Participant or Authorized User, or the adequacy or integrity of System safeguards.

### **Participant Cooperation**

Each Participant shall cooperate with CyncHealth in any investigation of CyncHealth or of another Participant into CyncHealth's or such other Participant's privacy and security compliance, whether conducted by an agency of state or federal government or conducted as a self-investigation by CyncHealth or the other Participant, when the investigation implicates such Participant's compliance with CyncHealth policies or the adequacy or integrity of System safeguards.

### **Application to BAs and Contractors**

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

If the CyncHealth Privacy Officer determines that PHI that was wrongfully used or disclosed is created or maintained by a business associate of CyncHealth, the CyncHealth Privacy Officer will notify the BA of the results of the investigation and any required action on the part of the BA. If the results of the investigation are that CyncHealth's BA misused or improperly disclosed an individual's PHI, the CyncHealth Privacy Officer will prepare a recommendation for the CyncHealth Board as to whether the business associate relationship between the BA and CyncHealth should continue.

### **Duty to Mitigate**

Each Participant shall implement a process to mitigate, and shall mitigate to the extent practicable, the harmful effects that are known to the Participant of an access, use or disclosure of Protected Health Information (PHI) or Personally Identifiable Information (PII) through the System that is in violation of applicable laws and/or regulations and/or these

Policies and that is caused or contributed to by the Participant or its workforce members, agents, and contractors. Steps to mitigate could include, but are not limited to, Participant notification to the individual or Participant request to the party who improperly received such information to return and/or destroy impermissibly disclosed information.

### **Mitigation by CyncHealth**

If an investigation of a privacy breach indicates that PHI was misused or improperly disclosed, the CyncHealth Privacy Officer shall determine:

1. what, if any, privacy practices at CyncHealth require modification;
2. whether a new policy, procedure, or form should be developed or whether an existing policy, procedure, or form should be revised;
3. whether additional training is required to avoid a repeat violation; and,
4. what sanctions, if any, will be imposed against the individual who committed the violation.

### **No waiver**

No individual will be asked to waive his/her rights, including the right to file a complaint about the use or disclosure of his/her PHI or PII.

### **Policy 1000: Information Security Policy**

The purpose of this policy and procedures is to provide a framework for the roles and responsibilities, expectations, and relationship between CyncHealth and its Participants with the goal of protecting and securing information assets. As such, this document will clarify responsibilities related to the security of CyncHealth's technology and information resources.

#### **Information Stewardship**

Participants shall protect the security and privacy of all information entrusted to them. Participants are expected to comply with these Policies in their use of the System as set forth in the Participant Agreement, 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.

#### **Information Standards**

Participants must send all available data elements included in the latest version of the United States Core information for Interoperability (USCDI) standards to meet the requirements of the Participation Agreement.

#### **Authorized User Controls**

##### Participant Responsibilities

Each Participant is responsible to:

1. Designate its responsible contact person who shall be initially responsible on behalf of the Participant for compliance with these policies and to receive notice on behalf of the Participant. For Participants that have their own system administrator, this shall ordinarily be the system administrator.
2. Designate its own Authorized Users from among its workforce, and designate BAs and contractors authorized to act as (or designate from among their workforce) Authorized Users on its behalf.



3. Train and supervise its Authorized Users and require any BA or contractor to train and supervise its Authorized Users consistent with these and the Participant's Policies and the BA Agreement as applicable.
4. The Participant shall take action to ensure that any Authorized Users who based on a change in job responsibility or employment status no longer qualify to access the System, are immediately removed from access to the System. Participant System Administrators (aka Designated User or Designated Authorizer), carry elevated role management functions and are directly responsible to action removal of provisioned users prior to, contemporaneously with or immediately following such a change so as to prohibit continued access authority for individuals who no longer need or qualify to access the System on behalf of the Participant in accordance with the terms of the Participation Agreement.
5. Hold their Authorized Users accountable for compliance with these and the Participant's policies and, as applicable, the terms of any BA Agreement.

#### CyncHealth Responsibilities

CyncHealth is responsible for:

1. Grant access authority to individuals designated by a Participant, subject to reserved authority to suspend, limit, or revoke such access authority as described later.
2. Train and supervise its own Authorized Users on these policies and the standard terms required by its BA Agreement with Participants.
3. Suspend, limit or revoke access authority for its own Authorized Users or any Authorized User who is a member of the workforce of any subcontractor of CyncHealth as required by these policies or the terms of its BA Agreement in the event of breach or non-compliance.

4. Immediately revoke access authority upon a change in job responsibilities or employment status of its own Authorized Users or the Authorized Users of any of its subcontractors.
5. Suspend, limit, or revoke the access authority of an Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's privacy policies, CyncHealth policies or the terms of the user agreement, if CyncHealth determines that doing so is necessary for the privacy of individuals or the security of the System.

### **Access Management**

As set forth in the Participation Agreement, Participant access to the Health Information Exchange (HIE) will be limited to the minimum necessary amount of Electronic Protected Health Information (ePHI), Personally Identifiable Information (PII), or Confidential Information.

### **Participant Security and Privacy**

Participants must maintain their systems in compliance with all applicable state, federal, Privacy Rule, and HIPAA regulations. For systems that directly interact with the CyncHealth System, Participants must maintain all systems, system components, system applications, and networks at an industry-accepted baseline standard to prevent unauthorized access to the System or a potential breach. CyncHealth and its Participants are committed to data security. In connection with HIE services, CyncHealth and Participants will use administrative, physical and technical security measures—such as access controls, authentication measures, auditing procedures and security incident reporting—that meet applicable legal requirements, security and reporting obligations in the Participation Agreement, and best security practices in the healthcare industry.

Participants must also follow CyncHealth's security protocols and related measures with respect to Participants' use of HIE services, such as minimum username/password requirements, authentication procedures, and access termination requirements. These

security measures are all directly related to safeguarding the confidentiality and integrity of information by mitigating the risk of access by unauthorized persons, see 45 C.F.R. 164 Subpart C.

### **Access Maintenance**

Participant 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.

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.

### **Downtime, Maintenance and Updates**

1. For the HIE to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that the HIE be taken offline or performance degraded temporarily. There may also be security incidents, serious environmental events, or information corruption/technical errors that give rise to a substantial risk of harm to individuals, that may require CyncHealth to take similar action with respect to the entire system or to specific Participants affected by a security or information corruption/technical error.
2. Consistent with CyncHealth's obligations in the Participation Agreement, Participants understand and acknowledge that the HIE may be temporarily unavailable, or

performance may be degraded temporarily, for any of the following reasons, including but not limited to:

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

### **Compliance**

The Participant is responsible for its own compliance with the terms of the Participation Agreement, HIPAA, the Policies, and any applicable state or federal law or regulations. 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.

### **Application to BAs and Contractors**

Participants shall make this policy applicable to their BAs and to the contractors and subcontractors of their BAs as they deem appropriate through the terms of their business associate agreements.

### **Policy 1100: Complaints About Uses and Disclosures of Confidential Information**

In accordance with HIPAA or Federal requirements, individuals may complain about how CyncHealth uses and discloses their confidential data including Protected Health Information (PHI) or Personally Identifiable Information (PII). All complaints regarding CyncHealth's conduct will be submitted to the CyncHealth Privacy Officer for investigation and resolution.

#### *Procedures*

#### **Submission of Complaints**

An individual may submit a complaint about the use or disclosure of PHI by CyncHealth to either CyncHealth using the online submission form at <https://app.mycompliancereport.com/report?cid=CYNC> or to the Secretary of the Department of Health and Human Services (HHS) in Washington, DC.

If the individual wants to file a formal complaint with CyncHealth, he/she should contact the CyncHealth Privacy Officer. If the individual wants to file his/her complaint with the Secretary of HHS, he/she should be directed to and follow the steps provided on the Office for Civil Rights website ([www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa)). Complaints regarding the use or disclosure of an individual's PHI by a CyncHealth Participant will be returned to the individual or government agency with an explanation that the complaint needs to be submitted directly to the Participant for investigation and resolution.

#### **Responsibilities of the CyncHealth Privacy Officer Upon Receipt of an Individual Complaint**

##### Documentation

The Privacy Officer will document each privacy complaint received including in the documentation a brief description of and/or the basis for the complaint.

### Investigation

With the assistance of CyncHealth support staff, the Privacy Officer will investigate to determine:

1. what, if any PHI was misused or improperly disclosed;
2. if PHI was misused or improperly disclosed, whether such misuse or improper disclosure violates these policies;
3. what, if any, privacy practices at CyncHealth require modification;
4. whether a new policy, procedure, or form should be developed or whether an existing policy, procedure, or form should be revised; and,
5. whether additional training is required to avoid a repeat violation.

### Resolution

If the Privacy Officer determines a violation has occurred, he/she will consult with CyncHealth staff and/or the Privacy Officer of the Participant whose staff inappropriately used or accessed PHI to determine what sanctions, if any, will be imposed against the individual who committed the violation.

The Privacy Officer will supplement the initial documentation to include documentation of the investigation and any actions taken in response to the complaint. All documentation relating to the individual's complaint will be maintained for a minimum of six (6) years. If the PHI that was wrongfully used or disclosed is created or maintained by a BA of CyncHealth, the CyncHealth Privacy Officer will:

- i. notify the BA of the results of the investigation and any required action on the part of the BA; and,
- ii. if the results of the investigation are that the BA misused or improperly disclosed an individual's PHI, prepare a recommendation for the CyncHealth Board as to whether the business associate relationship between the BA and CyncHealth should continue.

#### Non-retaliation for Filing a Complaint

CyncHealth will not intimidate, threaten, coerce, discriminate, penalize, or take other retaliatory action against an individual who exercises his/her rights under HIPAA or Federal requirements or against any individual who participates in a process governed by the Privacy Regulations. This prohibition also applies to:

1. individual and/or individual complaints filed with the Secretary of HHS;
2. testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing arising under the HIPAA or Federal Privacy Regulations; or,
3. opposing any act or practice of CyncHealth, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not disclose PHI in violation of the HIPAA or Federal Privacy Regulations.

#### No waiver

No individual will be asked to waive his/her rights, including the right to file a complaint about the use or disclosure of his/her PHI or PII.

#### Questions

Questions about filing a complaint with CyncHealth or the Secretary of HHS should be directed to the Privacy Officer.

**Policy 1200: Breach Notification**

In the event a Participant determines that data transmitted through CyncHealth has been requested, used, or disclosed by Participant or an Authorized User in a manner that does not comply with Applicable Law and/or the provisions of the Participation Agreement, Participant must notify CyncHealth of the event. Notification should include a detailed summary of the relevant facts, within two (2) business days of the determination. Participant will cooperate with CyncHealth as to further investigation or responsive action reasonably requested or taken by CyncHealth to respond to the event. The notification shall be treated by CyncHealth as Confidential Information, except as otherwise required pursuant to Applicable Law or as used or disclosed by CyncHealth in connection with the exercise of CyncHealth's rights and/or obligations under the Participation Agreement to defend its actions in any process or the proceeding begun by or involving the Participant or Applicable Law.

In the event that CyncHealth determines that Participant data transmitted through CyncHealth has been requested, used or disclosed by CyncHealth in a manner that does not comply with Applicable Law and/or the provisions of the Participation Agreement and that such event constitutes a breach, CyncHealth will comply with the provisions of the applicable Business Associate Agreement.

In the event of a breach of unsecured Protected Health Information (PHI) or Personally Identifiable Information (PII) through the System, CyncHealth will fully cooperate with the Participant(s) who is the owner/creator of the disclosed information and any Participant(s) who may be involved in the incident to provide proper breach notification in compliance with the Breach Notification Requirements of the Business Associate Agreement and any other applicable federal or state notification law including 45 CFR Part 164 Subpart D. Procedure.



Any CyncHealth Participant, Authorized User, employee, contractor, or agent who discovers or suspects that a breach of patient information has occurred through the System will immediately notify the CyncHealth Chief Information Security Officer (“CISO”). Notification may be made by e-mail, [security@cynchealth.org](mailto:security@cynchealth.org).

The CyncHealth CISO will log the report and, in conjunction with the CyncHealth Privacy Officer, take any necessary action to promptly investigate and if necessary, mitigate the situation, and/or reduce the likelihood of any further breach.

In addition, the CyncHealth CISO will:

1. As set forth in the Business Agreement, notify the Participant who is the owner/creator of the disclosed information and any Participant(s) who may be involved in the incident;
2. identify the individuals whose unsecured PHI has been, or is reasonably believed to have been breached;
3. promptly investigate the circumstances and nature of the breach; and,
4. if necessary, conduct a risk assessment to determine whether the disclosure poses a significant risk of financial, reputational, or other harm to the individual and whether any exception to the breach rules apply.

#### *Risk Assessment*

For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is otherwise permissible and occurs despite reasonable safeguards and proper minimum necessary procedures would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification, a risk assessment must be performed to determine if there is significant risk of harm to the individual because of the impermissible use

or disclosure. This risk assessment must comply with 45 CFR 164.402 (2) and shall be documented as part of the overall investigation.

The risk assessment and the supporting documentation shall be fact specific and consider to whom the information was impermissibly disclosed, the type and amount of PHI involved, and the potential for significant risk of financial, reputational, or other harm.

#### *Notification*

Upon determination that breach notification is required, the notice shall be in accordance with applicable state and federal laws including 45 CFR Part 164 Subpart D. CyncHealth and the Participant(s) whose patient and/or information is affected will work together to review and approve the language of any notification required to be provided by the Participant as a Covered Entity under 45 CFR Part 164 Subpart D.

#### *Notice to Secretary of HHS*

1. Each impacted Participant Covered Entity, shall provide Notice to the Secretary of HHS when the breach of unsecured PHI of more than five hundred (500) patients from a single state is accessed, acquired, used, or disclosed.
2. For breaches involving less than five hundred (500) individuals from a single state, a log of the breaches shall be maintained and annually submitted by the Participant Covered Entity to the Secretary of HHS.

#### *Retention of Records*

CyncHealth shall retain all documentation related to the breach investigation, including the risk assessment, for a minimum of six years.

## **Policy 1300: Insurance Requirements**

### **Required Coverage**

CyncHealth shall maintain, throughout the term of the Participation Agreement, at its sole expense, insurance for “cyber-liability” or similar insurance appropriate to a breach of Information, as well as such professional and general liability insurance coverage as it deems reasonable and necessary to insure itself and its officers, directors, and employees against any third-party claim or cause of action arising out of the performance of the Participation Agreement.

#### Participant Coverage

Each Participant shall maintain, throughout the term of its Participation Agreement, at its sole expense, such professional, general, and cyber liability insurance coverage as it deems reasonable and necessary to insure itself and its officers, directors, and employees against any third-party claim or cause of action arising out of the performance of its Participation Agreement.

#### Survival

In the event of termination of the Participant’s Participation Agreement for any reason, CyncHealth and each Participant either shall maintain its insurance coverage called for under this Policy for a period of not less than three (3) years or shall provide an equivalent extended reporting endorsement (“tail policy”).

#### *Evidence of Coverage*

CyncHealth and each Participant shall provide proof of such required coverage upon request.

CyncHealth will not add the Participant as a named insured.

*Commercial or Self-Insurance*

The insurance coverage required under this Policy may be provided through one or more commercial insurance policies through a self-insurance fund reasonably satisfactory to CyncHealth, or through a combination of commercial and self-insurance.

### **Policy 1400: Privacy and Security Governance**

Privacy and Security management shall be overseen by the Compliance and Cybersecurity Committee of the CyncHealth Board and managed by the CyncHealth Privacy Officer and Security Officer. The Compliance and Cybersecurity Committee shall be responsible for reviewing privacy and security policies and making recommendations to CyncHealth management and Board of Directors.

#### **Responsibilities**

Members of the Compliance and Cybersecurity Committee shall be appointed by and report to the CyncHealth Board. The Compliance and Cybersecurity Committee shall be responsible for providing overall direction and management regarding privacy and security and this Plan. Specifically, the Compliance and Cybersecurity Committee shall:

1. Make recommendations to the Board with regard to privacy, confidentiality and security policies and practices.
2. Review and recommend modification of privacy, confidentiality and security policies and practices in light of operating experience, changes in law, and changes in available compliance tools.
3. Advise on privacy, confidentiality and security awareness and training initiatives to educate workforce and users about risks.
4. Review the summary of the findings from risk assessments and audits of information systems and privacy and confidentiality practices.
5. Maintain working relationships with the privacy and security officers and managers of the institutions participating in CyncHealth.
6. Represent a cross-section of the CyncHealth Participants representing their geography, size and type of covered entity.

## Policy 1500: Privacy Officer

The Privacy Officer shall be responsible for the operational aspects of Privacy. The Privacy Officer shall have authority commensurate with his or her responsibilities.

### Responsibilities

The Privacy Officer is appointed by the Board and reports to the Compliance and Cybersecurity Committee and the Chief Legal Officer. The Privacy Officer is responsible for operational matters regarding the implementation of the Privacy Policies and related privacy matters. Specifically, the Privacy Officer:

1. Exercises responsibility for the development, implementation, management, and enforcement of privacy directives as mandated by the Compliance and Cybersecurity Committee, the Privacy Policies, HIPAA/HITECH and applicable state law.
2. Monitors changes to state and federal privacy laws and analyzes new privacy regulations, for impact on CyncHealth operations.
3. Reviews and recommends modification of the Privacy Policies and all supporting policies and procedures in light of operating experience, changes in applicable privacy laws, and changes in available compliance tools.
4. Is responsible for implementing, managing, and enforcing privacy directives as mandated by the Compliance and Cybersecurity Committee, the CyncHealth Privacy Policies, HIPAA/HITECH and applicable state law.
5. Documents and monitors CyncHealth's relationship specifically as a business associate to covered entities and subcontractors participating in CyncHealth to ensure contractual requirements are in compliance with the HIPAA business associate agreement requirements of HIPAA and Applicable Law.

6. Manages the ongoing integration of privacy protections with business strategies and requirements.
7. Participates in ongoing information risk assessments and audits to ensure that privacy is adequately protected and meets Applicable Laws.
8. Works with vendors, outside consultants, and other third parties to improve privacy practices within the organization.
9. Participates on the incident response team to contain, investigate, mitigate and prevent future privacy incidents or breaches.
10. Is designated to receive privacy complaints and respond to questions from Participants and third parties regarding CyncHealth's privacy practices.
11. Works cooperatively with other applicable organization units to oversee responses to requests by entities or individuals for access to Information as appropriate to the situation.
12. Monitors a database of privacy-related complaints, patient Information access requests, Participant audit requests, business associate agreements and other privacy-related documentation.
13. Monitors the effectiveness of the Privacy Policies and incorporates the results of monitoring into recommendations for amendment, sanction or other action.
14. Works with Human Resources in developing and implementing sanctions as appropriate for issues of non-compliance.

15. Assures timely and effective HIPAA Privacy training and retraining of the workforce.
16. Uses judgment in assessing exposure, recommending solutions, and overseeing compliance with the Privacy Policies.
17. Maintains working relationships with legal counsel and outside consultants and as authorized by the CyncHealth Executive Committee, uses the services of such parties to assist with implementing the Privacy Policies.
18. Maintains working relationships with the privacy and security officers and managers of the institutions participating in CyncHealth.

#### Qualifications

The Privacy Officer should possess the following qualifications:

1. Outstanding interpersonal and communication skills.
2. Excellent management skills.
3. Experienced in the field of health information management and information technology.
4. Understanding of corporate compliance and organizational improvement processes.
5. Must possess a high degree of integrity and trust along with the ability to work independently.
6. Ability to weigh business risks and enforce appropriate privacy measures.
7. In-depth knowledge of the HIPAA Privacy Rule and other applicable state and federal privacy laws.



8. Experience in health care operations.

#### Personal Skills

The Privacy Officer should possess the following personal skills:

1. Excellent leadership skills and communication skills.
2. Willingness to become an organizational resource on HIPAA/HITECH and other applicable state and federal privacy laws.

#### Project Management Skills

The Privacy Officer should possess the following project management skills:

1. Compliance and Cybersecurity

### **Policy 1600: Information Access Management**

CyncHealth shall grant Participants access to the HIE as set forth in the Participant Agreement and these Policies. Such access will be limited to the minimum necessary amount of Electronic Protected Health Information (“EPHI”).

### **Procedures**

#### *Access Authorization and Establishment*

1. CyncHealth will require the assistance of technical specialists from time to time to develop and maintain CyncHealth's system. These people should have limited ongoing access monitored by the Security Officer.
2. Applications shall incorporate controls for managing access to selected information and functions, including auditing capabilities. Exception: GoDaddy hosted websites are accessed using a shared account.
3. Each user of the system should have a unique identification. The system should provide a method to accurately identify the user through a two-factor authentication process.<sup>3</sup> All systems should include identity authentication functions that are consistent with this policy and with the level of confidentiality of the information they contain or process. Exception: GoDaddy hosted websites are accessed using a shared account.
4. The authority and ability to read, write, modify, update and/or delete information from automated files or databases should be established by the Security Officer, Program Director and System Administrator. Users may be granted a specific combination of authorities and abilities. Users should not be given any authority or ability beyond their needs. Access rules or profiles should be established in a manner that restricts users

---

<sup>3</sup> Two-factor authentication requires factors beyond general usernames and passwords to gain access (e.g., requiring users to answer a security question such as “Favorite Pet’s Name”) as defined in the HIPAA Security Guidance bulletin from the Centers for Medicare & Medicaid Services (CMS) on December 28, 2006

from performing incompatible functions or functions beyond their responsibility and enforces a separation of duties.

5. Computer operations which support sensitive information shall operate in accordance with procedures approved by the Security Officer and assure that:
  - A) information cannot be modified or destroyed except in accordance with procedures;
  - B) operating programs prohibit unauthorized inquiry, changes or destruction of records; and,
  - C) operating programs are used to detect and store all unauthorized attempts to penetrate the system.

**Appendix F**

<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.		

**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.		

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.

**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.

2. 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.

3. 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.

4. 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.

5. 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;

Capitalized terms not otherwise defined herein shall have the meanings assigned to them in the HIPAA regulations.

**DISCLOSING INFORMATION TO 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.		

**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.

3. 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.

4. 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:

5. 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:

- 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
- The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

C. 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

D. 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.

<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.		

## USING AND DISCLOSING OF HEALTH INFORMATION

### 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.		

Other requirements	Notes	Check-off
(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 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).		
(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.		

**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.		

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.		

#### 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.		

### 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> Redisdisclosure 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.		

### 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).

### 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

### Patient Opt-Out Procedure

<b>Procedure:</b> Patient 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 patient 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
    - First Name \*
    - Last Name \*
    - Middle initial \*
    - Date of Birth \*
    - Address
    - Phone number
    - Facilities visited

b. Webform: via [Opt In/Out \(teamdynamix.com\)](http://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


g.

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

i.



- h. Set Consent Value Field to 0 for Opt out or 1 for Opt In.
  - i. Set Status to Pending Provisioning.
  - j. 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 notating that it was processed and validated.
6. Once all patients are Processed, the .csv can be moved to the "completed" subfolder.

### 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.		

#### 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.