CyncHealth

Governing Principles and Policies

CyncHealth

We are on a mission to empower healthier communities through steadfast pursuit of advancing interoperability, bringing data democratization, cultivating economic value, and delivering a health data utility.

CyncHealth

Contents

CyncHealth Governing Principles and Policies

INTRODUCTION

The following policies apply to the access, use, and disclosure of Protected Health Information (PHI) or Personally Identifiable Information (PII) by Participants (collectively referred to as "Information") 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 Governing Principles and 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. CyncHealth reserves the right to make changes to the Policies. Notice of changes may be provided by posting the amendment, along with its effective date, on the CyncHealth website www.cynchealth.org, as well as providing written notice via email to Participant, if such changes are material.

CyncHealth has incorporated the specific flow-down provisions related to CyncHealth's contractual arrangements with other HIEs and data analytics vendors that impact the Policies.

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 CYNCHEALTH 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 privacy 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.

SAFEGUARDS IN AN ELECTRONIC NETWORKED ENVIRONMENT

HIPAA permits covered entities that hold protected health information to disclose such information to third parties for the disclosing entity's own treatment, payment, and health care operations. HIPAA also permits covered entities that hold protected health information to disclose such information to other covered entities (or providers in the case of treatment) for the receiving party's treatment, payment, or health care operations.

In an electronic networked environment, such as the System, the disclosing Participant will not receive or "process" a request for disclosure. The other Participant that needs the information, using the System, can simply locate the Participant's records and access them as needed. The human element of analyzing individual requests is absent.

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"[1] health care operations of the receiving Participant and in compliance with these Policies (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

In all cases, access and disclosure are 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

[1] 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.

they are the payment or health care operations of the disclosing or receiving Participant, these conditions and safeguards include meeting the minimum necessary standard.

Policy 100: Compliance with Law and Policy

Scope and Applicability

This Policy applies to CyncHealth and all Participants.

Policy

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 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

This Policy applies to all Participants.

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[2] 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."*

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

[2] C.F.R. § 164.520(b). See 45 C.F.R. § 164.520(c)(2)(ii).

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

Scope and Applicability

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

Special Protection

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.

CyncHealth

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

Definitions

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.

Scope and Applicability

This Policy applies to CyncHealth and all Participants.

Policy

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 thirty (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;
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

Scope and Applicability

This Policy applies to CyncHealth and all Participants.

Policy

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 de-identified data for other purposes, transfer it to third parties for other purposes, re-identify the de-identified 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 five 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

Scope and Applicability

This Policy applies to CyncHealth, all Participants and their BAs and contractors.

Policy

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

This Policy applies to CyncHealth and all Participants and their BAs and contractors.

Policy

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 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 workforces.

Policy 700: Individual Rights to Access to Health Information

Scope and Applicability

This Policy applies to CyncHealth and all Participants.

Policy

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. 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, 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

Scope and Applicability

This Policy applies to CyncHealth, all Actor Participants and their BAs and contractors.

Policy

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 21st 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.

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

This Policy applies to CyncHealth, all Participants and their BAs and contractors.

Policy

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

Scope and Applicability

This Policy applies to CyncHealth, all Participants, and their BAs and contractors.

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, unless provide a written exemption from CyncHealth.

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. Ensure the training of 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, which 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 ques 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

Scope and Applicability

This Policy applies to CyncHealth and all Participants.

Policy

In accordance with HIPAA or Federal requirements, individuals may complain about how CyncHealth uses and disclose 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). 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

Scope and Applicability

This Policy applies to CyncHealth and all Participants.

Policy

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.

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.

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

Scope and Applicability

This Policy applies to CyncHealth and all Participants.

Policy

Required Coverage

CyncHealth 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 1600: Information Access Management

Scope and Applicability

This Policy applies to CyncHealth and all Participants.

Policy

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.[3] 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 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.

[3] 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