CliniSync Policy Manual

The Ohio Health Information Partnership Board of Directors governs the CliniSync Health Information Exchange (HIE) and Directed Exchange Services and approves all changes to the CliniSync Policy Manual. All entities participating in CliniSync are required to follow the policies contained in this manual. The policies provide baseline requirements for the CliniSync and are the foundation for the development of additional procedures and implementation guides. The creation of new policies and changes to existing policies will be implemented following the process identified in the Scope Policy. All employees and contractors of the Ohio Health Information Partnership will be required to comply with the HIPAA Policies and Procedures in addition to the CliniSync Policy Manual.

Revision History

Section	Revision History
A. Definitions	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions approved 2/22/13 -Revisions Approved 1/19/2018
B. Scope	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 1/19/2018
C. Participant Requirements	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 1/19/2018
D. Patient Consent Policy	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 8/7/15 -Revisions Approved 11/13/15 -Revisions Approved 12/11/15 -Revisions Approved 1/19/2018
E. Permitted Use	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12

	-Revisions Approved 2/22/13 -Revisions Approved 6/12/15 -Revisions Approved 1/19/2018
F. Audit Policy	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 12/11/15 -Revisions Approved 1/19/2018
G. Authorization Policy	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 1/19/2018
H. Authentication Policy	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 1/19/2018
I. Patient Information Request Policy	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 1/19/2018
J. Security Policy	-Original Policy Approved 6/24/11 -Revised per Operational Review 11/18/11, 10/25/12, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 1/19/2018
K. Violation/Breach of CliniSync Policies or Participant Agreement	-Original Policy Approved 6/24/11, 11/9/12 -Revisions Approved 2/22/13 -Revisions Approved 1/19/2018
L. Exchange of Restricted Health Information	- Original Policy Created by 2012 Behavioral Health Task Force -Approved 2/22/13 -Revisions Approved 1/19/2018
M. Participant Obligations Under the Data Use and Reciprocal Agreement Policy	- Policy Approved 10/25/13 - Revisions Approved 1/19/2018

N. HISP Provider Directory	-Policy Approved 10/16/14 -Revisions Approved 1/19/2018
O. Data Correction and Deletion Policy	-Policy Approved 6/12/15 -Revisions Approved 1/19/2018
P. Notification Services Policy	-Policy Approved 6/12/15 -Revisions Approved 8/11/17 -Revisions Approved 1/19/2018
Q. Notification and Clinical Exchange Services for Organizations Managing Populations	-Policy Approved 8/11/17 -Revisions Approved 1/19/2018

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Definitions
Date of Board Approval: February 22, 2013
Applicable Services: Direct Exchange Services and HIE Services

A. Definitions

Background:

The following definitions apply to the use of services offered by CliniSync.

Policy:

Any term that is defined in the HIPAA Privacy Regulations, 45 CFR §160.103, and included in this manual shall maintain the definition given to it in the regulation. The following terms are used throughout the CliniSync Policies and will have the definitions identified below.

1. **Affiliated Practitioner**: A Practitioner employed by or under contract to a Participating Organization to provide health care services to the Participating Organization's patients, a Practitioner on a Participating Organization's formal medical staff or a Practitioner providing services to a Participating Organization's patients in a cross-coverage or on-call arrangement.
2. **Applicant User**: An individual applying to become an Authorized User of CliniSync. A Participating Organization.
3. **Authorized User**: includes any employee, contractor or medical staff member of a Participating Organization or any of its Affiliated Practitioners authorized by the Participating Organization to access and use CliniSync under this Agreement.
4. **Audit Log**: A record of the information from successful and unsuccessful queries of the HIE. The specific components of the audit log are identified in Section F. CliniSync Audit Policy.
5. **Business Associate Agreement**: A written signed agreement meeting the HIPAA requirements of 45 CFR §160.103.
6. **Covered Entity:** Shall have the meaning set forth at 45 CFR §160.103 of the HIPAA privacy rule.
7. **CliniSync Advisory Council**: Advisory Board created by the Ohio Health Information Partnership composed of at least one Long Term Care Organization, Lab, Behavioral Health Agency and regional representation from Participating Organizations.
8. **CliniSync**: The statewide Health Information Exchange (HIE) and Direct Exchange Services run by the Ohio Health Information Partnership.
9. **CliniSync Vendor**: The vendor(s) selected by the Ohio Health Information Partnership to provide technical HIE and Direct Exchange services.
10. **Health Care Provider**: A professional health care provider licensed by the state to provide health care services or otherwise authorized by the state to provide health care services.

11. Direct Exchange Services (DES): The ability for an Authorized User to initiate a transmission of Health Information to by means of electronic transmission of health information through a connection between the electronic systems of health care entities without the use of a Health Information Exchange (HIE). Direct Exchange includes but is not limited to the following processes:
    a. Health Information Services Provider (HISP)
    b. Results Delivery
    c. Referrals
    d. Notification Services for Providers of Care
    e. Services for Organizations Managing Populations
12. Health Care Operations: Shall have the meaning set forth at 45 CFR §164.501 of the HIPAA privacy rule.
13. Health Information Exchange (HIE) Services: "Health information exchange" means any person or governmental entity that provides a technical infrastructure to connect computer systems or other electronic devices used by covered entities to facilitate the secure transmission of health information through a request for information initiated by a query by an Authorized Participant. The Community Health Record is the HIE Service of CliniSync.
14. Health Information Exchange Consent (HIE Consent): An individual's consent to allow their health records to be shared through CliniSync HIE Services.
15. Health Plan: Shall have the meaning set forth at 45 CFR §164.103 of the HIPAA privacy rule.
16. HIPAA: The standards for privacy of individually identifiable health information and the security standards for the protection of electronic protected health information (45 CFR Parts 160,162 and 164) set forth by the U.S. Department of Health and Human Services under the "Health Insurance Portability and Accountability Act of 1996," as amended by HITECH, as in effect on the date of this Agreement and as may be amended, modified or renumbered.
17. HIPAA Policies and Procedures: The policies and procedures adopted by the Ohio Health Information Partnership to protect the privacy and security of PHI accessed by its workforce.
18. HITECH: The "Health Information Technology for Economic and Clinical Health Act of 2009" (part of the American Recovery and Reinvestment Act of 2009(ARRA)), and any of its implementing regulations.
19. Hybrid Entity: Shall have the meaning set forth at 45 CFR §164.504(a) of the HIPAA privacy rule.
20. Limited Participating Organizations: Organizations, which may or may not be Covered Entities that are approved by Partnership Staff to have limited use of CliniSync through the use of the CliniSync Referral Tool only. Limited Participating Organizations are considered "Participants" for this limited access, and are subject to various policies as "Participants" but are not otherwise permitted to use or access the CliniSync HIE Services. Limited Participating Organizations must abide by the "Limited Participating Organizations Policy."

21. Master Patient Index (MPI): A database that maintains a unique index (or identifier) for every patient registered at a Participating Organization.
22. eHealth Exchange: The eHealth Exchange is a set of standards, services and policies that enable secure health information exchange over the Internet. The network will provide a foundation for the exchange of health information across diverse entities, within communities and across the country, helping to achieve the goals of the HITECH Act.
23. Participant Agreement: The agreement made by and between the Ohio Health Information Partnership and each Participating Organization, which sets forth the terms and conditions covering the operation of the DES or HIE Services provided and the rights and responsibilities of the Participant and the Ohio Health Information Partnership.
24. Participating Organization (also *Participant*): An organization that has entered into a Participation Agreement with CliniSync. A Participating Organization must be a Covered Entity as defined by HIPAA.
25. The Partnership: The Ohio Health Information Partnership.
26. PHI: See *Protected Health Information.*
27. Practitioner: An individual licensed in the United States to practice medicine.
28. Protected Health Information (PHI): Shall have the same meanings as set forth in 45 CFR §160.103.
29. Query: Action by an Authorized User who has an established treatment relationship with a patient searching for clinical information for that patient that is available through CliniSync's HIE Services.
30. Restricted Health Information: Categories of health information that have special protections per state or federal law and/or subject to more stringent policies when exchanging through CliniSync.
31. Treatment: Shall have the meaning set forth at 45 CFR §164.501 of the HIPAA privacy rule.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Scope
Date of Board Approval: February 22, 2013
Applicable Services: **Direct Exchange Services and HIE Services**

B. Scope Policy

Background:

This policy explains the scope of the CliniSync Policy Manual. The Partnership will implement a range of policy and technical safeguards to protect and facilitate the exchange of protected health information. This policy identifies entities that are required to abide by the CliniSync Policy Manual and the process to amend these policies.

Policy:

1. Entities covered by the Policies and Procedures

The Partnership, in its sole discretion, shall define and distribute minimum mandatory policies to maintain the privacy, security, confidentiality, integrity and availability of CliniSync. The policies apply to following groups:

a) The Partnership and its Employees;

b) CliniSync Vendor(s); and

c) Participating Organizations, including their Authorized Users.

The Partnership will provide written procedures and implementation guidance for Participating Organizations.

Failure to comply with CliniSync Policies may result in sanctions against the non-compliant Participating Organization or Person. These sanctions are identified in the Participant Agreement signed by Participating Organizations and in Policy K. Violation/Breach of CliniSync Policies.

2. Information disclosure

CliniSync is only to serve as an intermediary among Participating Organizations for exchange of information for treatment, payment and health care operations. The Partnership will not disclose PHI for any reason except as required by law or as otherwise expressly permitted by a Participant in the Business Associate Agreement.

3. Process for Amending the Policies and Procedures

The Policy Manual is subject to an annual amendment process in which proposed changes will be solicited, evaluated and implemented as appropriate through a policy amendment process recommended by the Partnership staff and approved by the Board of Directors.

4. Accounting for discrepancies between the Participant Agreement and Policy Manual

If a discrepancy exists between the Participant Agreement and the Policy Manual, the terms of the Participant Agreement supersede the Policy Manual.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Participant Requirements
Date of Board Approval: February 22, 2013
Applicable Services: **Direct Exchange Services and HIE Services**

C. Participant Requirements Policy

Background:

This policy identifies general requirements for all organizations that wish to use the CliniSync HIE.

Policy:

1. Executed Documents Required For Participation

A Participating Organization will be required to execute a Participant Agreement, which includes the following documents.

a) The CliniSync Business Associate Agreement

b) Exhibit that includes a listing of all facilities wholly owned by the parent signatory.

The above listed documents will outline the obligations required of Participating Organizations if they choose to exchange data using CliniSync and are not subject to negotiation. Procedures and implementation guidance will be produced by the Partnership staff and disseminated to Participating Organizations during the provisioning phase.

2. CliniSync Policies

The Ohio Health Information Partnership and each Participating Organization will comply with this Policy Manual in its entirety. If the CliniSync Policies are amended, reasonable efforts to notify will be submitted to each Participating Organization. Each Participating Organization is responsible for ensuring it is in possession of and in compliance with the most recent CliniSync Policy Manual. The Policy Manual and additional procedural documentation will be available on the CliniSync website operated by The Partnership.

3. Participating Organization Policies

Each Participating Organization must, at all times, comply with all applicable federal and state laws and regulations including, but not limited to, those protecting the confidentiality and security of PHI and those establishing individual privacy rights. Participating Organizations are also required to comply with updates to interpretations of such law and regulations. Participating Organizations must be aware of the provisions of certain state laws that are more

stringent than, and not preempted by, the HIPAA Privacy and Security Regulations.

4. Hybrid Entities

A Participating Organization may have an operational unit that acts as a Covered Entity as defined by HIPAA and an operational unit that does not have Covered Entity status. In these cases, the operational unit that is considered a Covered Entity may participate in CliniSync but the non-Covered Entity may not. The organizational unit that is a Covered Entity and uses the information cannot share any information obtained through CliniSync with the organizational unit that is not a Covered Entity as defined by HIPAA.

5. Privacy Officer

In accordance with HIPAA, all Covered Entities must have an identified Privacy Officer. CliniSync may sponsor supplemental privacy and security trainings for all interested users.

6. Site Administrator

All Participating Organizations are required to have a Site Administrator. The Site Administrator may or may not be the organization's Privacy Officer. The Site Administrator is responsible for performing duties related to user authentication, determining user's role based authorization, and notifying CliniSync in instances of improper use as defined by CliniSync policy. The Site Administrator will be the main point of contact between the Partnership and the Participating Organization.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Patient Consent Policy
Date of Board Approval: February 22, 2013
Applicable Services: HIE Services

D. Patient Consent Policy

Background:

This policy outlines the consent requirements for the query of an individual's PHI using the CliniSync HIE. There are no consent requirements required by the Partnership to use CliniSync for the Direct Exchange of PHI. Direct Exchange assumes that both the sender and the receiver have the appropriate authority and consent, if required, to share the information in question. In Direct Exchange, the sender is sending information to a recipient regarding a patient with whom the recipient has a direct relationship, such as a treatment relationship. For example, when a Health Care Provider sends a summary of a care episode to a referring Health Care Provider, they are using Direct Exchange to transfer PHI. The same is true when a lab delivers a result to the Health Care Provider who ordered it. It is implied in the fact that the Health Care Provider ordered the result that he should have the right to view the results to treat his/her patient.

The Office of the National Coordinator for Health IT released the Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap, FINAL Version 1.0. In the Roadmap, the ONC's position on consent for exchange through an HIE is evolving in part due to the need to coordinate with the diverse state laws on this issue throughout the country. However, the ONC notes that under federal law PHI can be shared for treatment, payment and health care operations, stating:

> "The HIPAA Privacy Rule generally permits the use or disclosure of PHI for limited specific purposes (such as treatment, payment and health care operations – often referred to as TPO) without an individual's permission. HIPAA Rules support electronic exchange of health information in an automatic way, with rules that run "in the background." This ensures our nationwide care delivery system continues to function. "[1]

Ohio Revised Code Chapter 3798 provides Ohio law governing health information exchanges ("HIEs"). The purpose of the new law, as stated in Chapter 3798.02 is: "to make the laws of this

[1] https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

state governing the use and disclosure of protected health information by covered entities consistent with, but generally not more stringent than, the HIPAA privacy rule for the purpose of eliminating barriers to the adoption and use of electronic health records and health information exchanges."

Policy:

1. General

A Participating Organization will comply with all applicable federal and state laws and regulations including, but not limited to, those protecting the confidentiality and security of PHI and establishing individual privacy rights. All Participating Organizations will comply with changes or updates to interpretations of such laws to ensure compliance.

If Query has been enabled at a Participating Organization, the Participating Organization must provide notice to patients and have a process to allow patients to choose not to participate, or opt out, as described in Section 6 below. Any information accessed by a Participating Organization through Query may remain part of the Participating Organization's records.

2. Consent Policies for Interstate Exchange

The consent policies set forth in this manual are the minimum policies required for exchange between the CliniSync HIE and those of other states. Other states may choose to implement less stringent policies for health information exchange within their state, but if their participants desire to exchange information with the CliniSync HIE, they shall comply with the Partnership's HIE Consent policy.

3. Consent Status

There are three different consent statuses available in the CliniSync System. The consent status affects an Authorized User's ability to query the CliniSync system. The different consent statuses are listed in sections 3.1-3.3.

3.1 Opted In by Default

A patient's consent status is set as opted in by default when they are first entered in the system, and may remain with this status unless the patient explicitly notifies either a Participating Organization or the Partnership of their desire to opt out of HIE.

3.2 Explicitly Opted In

A patient who has been given a chance to choose to have their information available in the CliniSync HIE and has affirmed that they would like to be included has a status of explicitly opted in.

3.3 Explicitly Opted Out

A patient who has been given a chance to choose to have their information available in the CliniSync HIE and has decided not to be included has a status of explicitly opted out.

4. Treatment Relationship

The CliniSync HIE technically monitors whether a Health Care Provider has a treatment relationship with a patient on whom they are searching or querying for information. Participating Organizations with a treating relationship for that patient may access the patient's information unless the patient has Explicitly Opted Out. A treatment relationship for purposes of accessing patient information is established in one of the following ways.

a) A Health Care Provider who is identified within a result or report message as the Ordering, Attending, Admitting, Consulting, Main Result Interpreter or Transcriptionist.

b) During the hospital registration, process the patient indicates their current treating Health Care Providers.

c) A Health Care Provider manually creates a relationship with a patient under their care manually within the CliniSync HIE.

d) A Health Care Provider creates a relationship within the Health Care Provider's electronic medical record.

5. Health Plan Enrollment Relationship

An enrollment relationship must be established prior to a Health Plan using CliniSync Direct Exchange Services. When a Health Plan submits a patient list to CliniSync it is confirming that this relationship exists. Other than what is permitted by Policy Q (Notification and Clinical Exchange Services for Organizations Managing Populations), clinical Protected Health Information will only be available to Health Plans from Participating Organizations who have executed an addendum permitting this release of this information.

6. Requirement to Provide Notice that a Participating Organization participates in Query-Based Exchange through an HIE

Participating Organizations who have enabled query are required to provide notice to patients of their participation in CliniSync HIE Services and a process to opt out.

6.1 Notice provided by Participating Organization

Each Query enabled Participating Organization must have an effective method to notify every patient for whom data is accessed of the Participating Organization's participation in the CliniSync Health Information Exchange.

This may be done by including the following components in the Participating Organization's Notice of Privacy Practices or other written notice that is presented to patients.

a) The fact that the Participating Organization participates in a Health Information Exchange where the patient's information can be shared and accessed.

b) Acknowledgement that the patient may opt out at any time and a description of the process of how to opt out.

Participating Organizations may also wish to include (but are not required to include) in this notice additional information such as (1) identifying CliniSync by name as an HIE in which the Participating Organization participates or (2) an explanation that opting out may result in medical information not being available through query even in an emergency.

7. Opting Out

A patient shall be entitled to opt out of CliniSync HIE Services by providing written notice to any Participating Organization with whom he or she has a provider/patient relationship. A Participating Organization is required to change the patient's consent status in the CliniSync system as soon as reasonably possible and no later than three business days of receipt of request. A patient may also contact the Partnership directly to change their consent status. If a patient has a consent status of Explicitly Opted Out (see Section 3.3 above) a Participating Organization cannot access that patient's information through the CliniSync HIE, even when the Participating Organization is a treating provider and even in the event of an emergency condition.

There are four ways a Participating Organization can execute a patient's decision to opt out. They are listed below.

1. The Participating Organization sends CliniSync a flag in their ADT message.

2. Participating Organization staff is trained on CliniSync Consent tool and logs in and changes consent status.

3. The Participating Organization sends CliniSync a support ticket requesting the patient be opted out.

4. The patient contacts CliniSync directly and completes and notarizes form available on website.

8. Minors

The CliniSync HIE contains minor PHI. It is the responsibility of the Participating Organization to ensure that a minor's consent is collected in a manner that is compliant with state and federal law. It is the responsibility of the Authorized User who accesses a minor's information from the HIE to be aware that a minor's information may be controlled by the minor and not his or her parent.

9. Exceptions to Consent status

The following activities are not impacted by consent status. Patient information may be used for the following activities regardless of consent.

9.1 Public Health

If the Participating Organization is required to disclose a patient's record to a government agency for purposes of public health reporting, the Partnership may make those disclosures through the CliniSync Direct Exchange Services on behalf of the Participating Organization regardless of consent status. This may occur under applicable state and federal laws and regulations.

These disclosures may include, but are not limited to: monitoring disease trends, conducting outbreak investigations, responding to public health emergencies.

9.2 Other Reporting as Required by Law

Other reporting required by state and federal law or as required by court order may be required regardless of consent status.

9.3 Master Patient Index

CliniSync may create a Master Patient Index regardless of consents status.

9.4 Direct Exchange Services

As noted in the Background section of this Policy, activities categorized as Direct Exchange are not controlled by a patient's HIE consent status.

Ohio law requires Covered Entities to allow patients to opt out of disclosures through an HIE. However, "direct exchange" services are expressly excluded from what constitutes "health information exchange" subject to ORC Chapter 3798. Because all Direct Exchange Services fall with disclosures for treatment, payment, or health care operations under HIPAA (see 45 CFR 164.506) and outside of "health information exchange" services under Ohio law (see ORC 3798.01), these disclosures may be made without patient consent.

10. Compliance with Existing Law

All access to PHI via the CliniSync HIE or Direct Exchange Services shall be consistent with applicable federal, state and local laws and regulations. If applicable law requires that certain documentation exist or that other conditions be met prior to accessing PHI for a particular purpose, Participating Organizations shall ensure that they have obtained the required documentation or met the requisite conditions.

11. Restricted Health Information

Restricted Health Information includes information with special protections per state or federal law. This type of information will not be available for query through the CliniSync HIE. A summary of information classified as Restricted Health information is included in Policy L: Exchange of Restricted Health Information. Restricted Health Information shared by patients with their Health Care Providers and included in progress notes may become part of that Health Care Provider's medical record and available for query.

12. Treatment and Coverage Not Conditioned on Consent

Participating Organizations must not condition treatment or coverage on the patient's willingness to provide access to the patient's information through the CliniSync HIE.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Permitted Use and Breach of Permitted Use Policy
Date of Board Approval: February 22, 2013
Applicable Services: **Direct Exchange Services and HIE Services**

E. Permitted Use Policy

Background:

The Permitted Use Policy will govern the purpose for which a patient's information may be retrieved by an Authorized User within a Participating Organization. This policy, when coupled with the Patient Consent policy, is designed to reduce unauthorized access and ensure that PHI is used only for authorized purposes.

Policy

1. Permitted Use

This section sets forth minimum standards that the Partnership and its Participating Organizations must follow to ensure that the information provided, accessed, made available, or otherwise processed through or by CliniSync (Data) is used only for permitted purposes. Consequences for violation of this policy and any other policy are included in Policy K. Violation/Breach of CliniSync Policies or Participant Agreement.

2. Permitted Use of Data by the Partnership

The Partnership employees and their contractors are required to comply with the Ohio Health Information Partnership HIPAA Policy and Procedures. The Partnership staff will limit their use of Data, and will require its contractors and agents to limit their use of Data, to those permitted uses outlined in the Participant Agreement, the CliniSync Policies and Procedures, and applicable laws. Specifically, the use of Data by the Partnership is limited to:

1. Access as required to operate and provide health information exchange services and/or otherwise permit Authorized Users to access Data through CliniSync or the eHealth Exchange.

2. Other access in compliance with applicable laws.

2.1 Aggregate Data

Any disclosure by the Partnership of Data for reasons other than the permitted uses described above will be limited to aggregated Data, de-identified in accordance with

HIPAA, except as may be required by applicable laws. The Partnership will not, without the prior written consent of a Participating Organization, disclose to any third party that any given Data contained within the aggregated Data originated from such Participating Organization, or included the identity of such Participating Organization within the aggregated Data.

3. Permitted Use of Data by Health Care Providers who are Participating Organizations

Participating Organizations will limit their use of Data to those permitted uses outlined in the Participant Agreement, the CliniSync Policies, and in compliance with applicable laws.

Specifically, without limiting the foregoing, the Participant Agreement limits the use of Data by Participating Organizations to uses in support of the Participating Organization's treatment of their own patients, payment for their health care services, and other uses as permitted by law and public health reporting.

4. Permitted Use of Data by Health Plans who are Participating Organizations

Other than what is permitted by Policy Q (Notification and Clinical Exchange Services for Organizations Managing Populations), a Health Plan will only have access to clinical Data from Participating Organizations who have signed an addendum to the Participant Agreement that permits their Data to be sent to Health Plans. A Health Plan is only permitted to use Data in accordance with HIPAA for payment and its own health care operations, as defined by HIPAA, so long as the Participant has or has had a relationship with the individual who is the subject of the information received, and the Participant uses the information only for quality assessment and improvement activities, including care coordination, or other purpose listed in paragraph 1 or 2 of the definition of health care operations in 45 CFR 164.501. For payment and health care operations purposes, a Health Plan shall use the minimum amount of Data necessary to accomplish their purpose. The Health Plan will only receive clinical Data from Health Care provider Participants who contractually agree to disclose to health plan participants. The Health Plan is not permitted to use the Data to deny insurance coverage or benefits to any individual.

5. Expressly Prohibited Uses of Participating Organizations

A Participating Organization may not access or use PHI or any proprietary information held by another Participating Organization to compare patient volumes, practice patterns, or make any other comparison, without that other Participating Organization's written approval. The Partnership shall not have access to use any Participating Organization's PHI on CliniSync unless expressly approved in writing by a Participating Organization or provided for by the Participant Agreement and Business Associate Agreement and with any required patient authorizations. Other uses of PHI (including but not limited to the CliniSync HIE and DES vendor reselling de-

identified data) are expressly prohibited under this policy without prior written approval from the Partnership and any Participating Organization whose data would be involved.

Unless approved in writing by the Partnership, Participating Organizations shall not utilize CliniSync to obtain the information of multiple people using a single automated process (e.g., batch processing, automated scripts, etc.). Without limitation to the foregoing, Participating Organizations may not utilize CliniSync in any manner that imposes an unusual data processing burden such that the efficient use of CliniSync by other Participating Organizations is impeded.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Audit Policy
Date of Board Approval: February 22, 2013
Applicable Services: HIE Services

F. Audit Policy

Background

This policy outlines the Audit requirements for the Partnership and Participating Organizations. Audits are useful oversight tools for recording and examining access to information and are necessary for verifying compliance with access controls. The goal of this policy is to prevent/limit inappropriate access to restricted information and to ensure that parties are adhering to policies and procedures required by CliniSync, state and federal law.

Policy

1. Information Required in Audit Log

An electronic Audit Log will be maintained by the CliniSync Vendor. These Audit Logs shall, at a minimum, include the following information:

[For successful queries:]

a) Identity of the patient whose information was accessed;

b) Identity of the Authorized User accessing the information; if the query is generated directly from an EMR for a Participating Organization the Authorized User Audit will be maintained by the Participating Organization.

c) Identity of the Authorized User's Participating Organization;

d) Location (internet address) from where the information or record was accessed if accessed from web portal;

e) Type of information or record accessed (e.g., pharmacy data, laboratory data, etc.);

f) Date and time of access (time must be recorded to millisecond accuracy); and

g) Source or location where the information is stored.

[For unsuccessful queries:]

a) Location (internet address) from where the unsuccessful access was attempted;

b) Date and time of unsuccessful access (time must be recorded to millisecond accuracy)

CliniSync may request from the CliniSync Vendor, at any time, an extract of various records from the Audit Log for various purposes including, but not limited to, verification of compliance with CliniSync policies, state and federal law, and release to authorized groups or individuals.

2. Immutability of Audit Log

Audit Logs shall be immutable. An immutable Audit Log requires either that log information cannot be altered by anyone regardless of access privilege or that any alterations are tamper evident. The CliniSync Vendor will, upon request, supply sufficient technical information to CliniSync to verify the integrity of the log and compliance with this requirement.

3. Retention of Audit Log

Audit Logs shall be retained for a period commensurate with the time period required by HIPAA and CliniSync.

4. CliniSync Audit of Participating Organizations

CliniSync will conduct periodic audits of the Audit Logs to ensure that all Participating Organizations are in compliance with the policies of CliniSync.

At a minimum, CliniSync shall audit the following:

a) Compliance with Policy D: Patient Consent;

b) Authorized Users who access information via CliniSync do so for Authorized Purposes, and

c) Role-based Authorizations are in place.

The activities of all or a statistically significant subset of CliniSync's Participating Organizations and their users shall be audited. These periodic audits of Participating Organizations shall be conducted at least on an annual basis.

5. Notice of Irregularities

Upon discovery of compliance irregularities during an audit, actions will be taken in accordance with the CliniSync Permitted Use and Breach Policy.

6. Participating Organization HIPAA Security Compliance

The Partnership will assist Participating Organizations with any HIPAA Security compliance processes required by a Participating Organization related to transfer of data through CliniSync. The Partnership's HIPAA Policies and Procedures are available to Participating Organizations on request. Each Participating Organization is solely responsible for its compliance with the HIPAA privacy and security regulations.

OHIO HEALTH INFORMATION PARTNERSHIP HIE POLICY
Subject: Authorization
Date of Board Approval: February 22, 2013
Applicable Services: Direct Exchange Services and HIE Services

G. Authorization Policy

Background:

Authorization is the process of determining whether a particular individual within a Participating Organization has the right to access CliniSync and to what information within the system they have access. Individual authorization will be determined by an individual's job function and scope. The job's function dictates the actions and outcomes required to perform the job and the job's scope identifies the information that is needed to complete the function. This type of authorization is also called role-based authorization. Furthermore, the currency and accuracy of user identification must be maintained to ensure that permissions are correctly set.

Policy:

1. Minimum Requirements

This policy sets forth the minimum requirements for the authorization of users, and is designed to limit exchange of information to the minimum necessary for accomplishing the intended purpose of the exchange. To ensure that patients have the utmost confidence in the privacy of their PHI as it moves through CliniSync, it is imperative that an individual's authorization does not exceed the level required to successfully perform their job.

2. User Requirements

All users that a Participating Organization grants access to query the CliniSync must abide by the following:

a) Each user has received or will receive training regarding the confidentiality of PHI under the HIPAA Privacy and Security Regulation and all other applicable federal and state laws and has signed a statement indicating awareness that they are obligated to protect PHI in compliance with these laws and CliniSync Policies;

b) Authorized Users may access the HIE only for purposes identified in the Participant Agreement signed by an individual's organization;

c) Authorized Users are obligated to keep confidential any passwords or other means for accessing the HIE and not to release them to any other individual.

3. Health Plan User Requirements

Health Plans may only grant employees of their organization access to CliniSync.

4. User Roles and Permissions

The CliniSync Vendor has a defined number of roles that can be assigned to Authorized Users. The list of system permissions needed to perform a given role is termed the "access profile." The CliniSync Vendor will supply a template of the access profiles for each role. Participating Organizations will add their users to the predefined templates provided by CliniSync as part of the provisioning process. Additional roles may be created depending on requirements of use cases.

5. Minimum Necessary Rule

Access profiles comply with the Minimum Necessary Rule pursuant to a Business Associate Agreement in accordance with HIPAA and are used to limit electronic access to PHI.

6. User Awareness of System / Information Access by Role

Participating Organizations will be responsible for specifying how job descriptions map to defined CliniSync User Roles. The Participating Organization is responsible for including information regarding access levels in training materials to assure that each user is aware of what system functions will be available and what information is permitted to be seen and used in their specific role/s. Users will also be made aware of access control policies and procedures, as well as system audit practices. The user is responsible for constraining their activities to the permission level granted by user role, organizational affiliation and patient authorization and reporting any discrepancies to the CliniSync Security Administrator. Any attempt to circumvent access restrictions will be viewed as a breach of security.

7. Modification/Termination of Access

If a user no longer requires system access, changes their role in the Participating Organization, or if system use audits demonstrate protracted inactivity or unauthorized activity in specific user accounts, modification or termination of access privileges will be processed by CliniSync as soon as possible and coordinated with the appropriate entities.

8. Review of Roles and Permissions Matrix

The user roles and permission matrix used to implement user access permission profiles will be reviewed and revised by the Participating Organization when a new role is created, when a role changes significantly, or when experience shows a need to make a modification. The Participating Organization will also ensure that the roles and permission matrix is reviewed at least annually to determine if the access granted to the various roles continues to be valid based on then-current business practices. All reviews will be documented and signed by an individual within the Participating Organization responsible for security of computerized data systems.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Authentication
Date of CliniSync Approval: February 22, 2013
Applicable Services: Direct Exchange Services and HIE Services

H. Authentication Policy

Background:

Authentication is the process of verifying that the individual requesting access to CliniSync is authorized to utilize CliniSync. This is accomplished both by technical and procedural means. The policies in this section represent an important safeguard for protecting patient information from internal and external risks and are designed to prevent, as far as possible, unauthorized access to the CliniSync system.

Policy:

1. General Policy

Each Participating Organization shall confirm each Applicant User's identity prior to that Applicant User obtaining access to CliniSync. The Participating Organization's confirmation of the Applicant User's identity will serve as an attestation that the Applicant User is both known to the Participating Organization and serves in a capacity which would allow access to CliniSync.

2. Minimum Authentication Required

Each Authorized User within a Participating Organization shall positively identify his or herself using, at a minimum, a unique user name and private password. The user name and initial password will be provided by CliniSync, or by a body otherwise identified in the Participant Agreement. While the Authorized User will have the ability to change the password, the user name will not be changeable.

Organizations are free to use more secure means of authentication (i.e., multi-factor authentication) to further protect against unauthorized access to the Organization's systems and CliniSync.

3. Site Administration

Each Participating Organization will name a Site Administrator, who may or may not be the Participating Organization's Privacy Officer under HIPAA rules. The identity and contact information of the Site Administrator will be registered with CliniSync. The Site Administrator is responsible for assuring the following:

a) Information provided to establish the identity of an Authorized Users is valid and accurate;

b) Authorized Users' professional credentials are current and valid; and

c) Assignment of Authorized Users' CliniSync roles is appropriate to users' job duties.

Designated users will be assigned permission to use CliniSync at the recommendation of the Participating Organization's Site Administrator.

4. Notification of Improper Use

The Site Administrator is responsible for immediately notifying CliniSync upon receiving knowledge of any improper activity, including misuse of authentication credentials, by an Affiliated User that could subject the Participating Organization, its patients or other CliniSync stakeholders to risk or harm.

OHIO HEALTH INFORMATION PARTNERSHIP HIE POLICY
Subject: Patient Information Requests
Date of OHIP Approval: February 22, 2013
Applicable Services: Direct Exchange Services and HIE Services

I. Patient Information Request Policy

Background:

Policy:

1. Release of Audit Logs to Patients

The Participating Organization shall provide patients, upon request, the Audit Logs pertaining to requests for their information.

The requested Audit Logs will contain, at a minimum, the following:

a) The name and role (e.g., physician) of each Authorized User from the Participating Organization who accessed a patient's Protected Health Information in the prior 6-year period;
b) The time and date of such access; and
c) The type of Protected Health Information or record that was accessed (e.g., clinical data, laboratory data, etc.).

2. Frequency of Release

The Participating Organization shall adopt policies pertaining to how often and at what charge a patient request for an Audit Log is fulfilled. All Participating Organizations policies related to patient request for an Audit Log must comply with state and federal law.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Security
Date of OHIP Approval: February 22, 2013
Applicable Services: Direct Exchange Services and HIE Services

J. Security Policy

Background:

The CliniSync Security Policy ensures that Participating Organizations observe all required privacy and security laws and regulations regarding securing PHI and the electronic PHI that is transmitted, received, maintained or stored in any form.

Policy:

1. General Policy

To ensure end-to-end security of information flowing through the CliniSync exchange, all Participating Organizations are required to confirm that they are HIPAA and HITECH compliant and specifically that they have met or exceeded all HIPAA Security obligations. This will ensure that Participating Organizations' individually identifiable health information is protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

2. Physical Environment

Participants shall maintain a secure environment for CliniSync-related infrastructure, services, and data to support the secure and reliable operation and continued development of CliniSync, including implementing and enforcing appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data accessed through CliniSync.

3. Security Controls

Participants shall employ security controls that meet applicable industry and Federal standards so that the information and data being transmitted shall not introduce any viruses, worms, unauthorized cookies, Trojans, malicious software, or "malware." In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.

4. Security Policies

Participants shall collaborate with CliniSync to develop security policies and to amend, repeal, or replace provisions as necessary to support the secure operation and continued development of CliniSync.

5. Security Reviews

A Participating Organization shall conduct periodic reviews, not less than once in a calendar year, of Participating Organization's internal security (for example, logs, access reports, and incident tracking), and make results of such review available to CliniSync.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Sanctions for Violation/Breach of Permitted Use
Date of Board Approval: February 22, 2013
Applicable Services: Direct Exchange Services and HIE Services

K. Sanctions for Violation/Breach of Permitted Use

This Policy is designed to hold violators accountable for violations of the CliniSync Policy Manual or Participant Agreement, to assure all Participating Organizations and patients of the Partnership's commitment to assure only permitted use of Data, and to mitigate the harm that any policy violation may cause.

Policy

1. Definitions of Violations and Breach

A violation of the CliniSync Policy Manual or Participant Agreement may be but is not limited to a HIPAA breach. This policy identifies sanctions for violation of the CliniSync Policy or Participant Agreement.

2. Notification of Violations by the Partnership

2.1 Notification of Violations

The Partnership will investigate any suspected or actual policy violation. This includes unpermitted access, use or disclosure of Data by the Partnership and its contractors and agents. The Partnership will notify any Participating Organizations if their Data is affected as a result of any unpermitted access, use or disclosure of its Data of which the Partnership becomes aware. This is outlined in the Partnership's HIPAA Policy and Procedure Manual.

3. Notification of Violations committed by Participating Organizations

3.1 Notification of Violations

Participating Organizations will notify The Ohio Health Information Partnership immediately if they become aware that they or any of their Authorized Users, contractors, or agents have accessed, used or disclosed Data for unpermitted purposes

and will take immediate and appropriate actions to cease any unpermitted access, use or disclosure of Data and to mitigate any resulting harm. Such Participating Organizations and their Authorized Users will be subject to the sanctions described in this policy in section 4.

In the event that the Partnership becomes aware, by whatever means, of improper access, use or disclosure of Data by a Participating Organization, the Partnership will notify the Site Administrator of the Participating Organization in accordance with the Partnership's HIPAA Policies and Procedures, and will require the Participating Organization to take immediate and appropriate actions to cease any unpermitted access, use or disclosure of Data and to mitigate any resulting harm.

4. Sanctions for Violations of CliniSync Policy Manual or Participant Agreement

The Partnership will establish appropriate sanctions that will apply to Participating Organizations and their Authorized Users in the event of their unpermitted access, use or disclosure of Data, and will apply or require its Participating Organizations to apply such sanctions, which will include but not be limited to:

a) Temporarily restricting an Authorized User's access to CliniSync;

b) Requiring Authorized Users to undergo additional training in the use of CliniSync;

c) Terminating the access of an Authorized User to CliniSync;

d) Suspending access of any Participating Organization to CliniSync for up to 14 days to investigate any potential improper access, use or disclosure of Data, or other violation of CliniSync Policies and Procedures or the Participant Agreement.

e) Temporarily restricting a Participating Organization's access to CliniSync;

f) Terminating a Participating Organization's participation in CliniSync; or

g) Such other remedies as CliniSync may reasonably deem necessary.

5. Dispute Resolution

Dispute resolution will follow the process identified in the contract signed by Participating Organizations.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Exchange of Restricted Health information
Date of Board Approval: February 22, 2013
Applicable Services: Direct Exchange Services and HIE Services

L. Exchange of Restricted Health Information

Purpose:

The purpose of this policy is to describe the categories of restricted health information that have special protections per state or federal law and/or are subject to more stringent policies when exchanging through CliniSync. Because restricted health information requires express written consent for disclosure per state and federal law, such as drug and alcohol records protected under federal statute (e.g., 42 CFR PART 2 REGULATIONS) or is subject to other restrictions on disclosures, participants must be aware of the guidelines and limitations of use for CliniSync's Direct Exchange and HIE Services.

Background:

Federal and state laws impose heightened restrictions on transferring certain records that disclose Protected Health Information that historically has been considered particularly private to a patient. Depending on the law, CliniSync Participants may be required to obtain patient authorization for the exchange of information by requesting that the patient sign a written document that contains certain elements.

While The Partnership wants to protect patients' privacy, there is general consensus among Health Care Providers that exclusion of certain sensitive health information could be detrimental to a patient's health and would preclude opportunities to improve outcomes as well as reduce costs. To assist, The Partnership convened behavioral health and legal experts through its Behavioral Health Privacy Task Force to recommend policies to encourage Participants to comply with the granular patient consent requirements for restricted data exchange.

Ohio Revised Code Chapter 3798 provides Ohio law governing health information exchanges ("HIEs") in Ohio. The purpose of Chapter 3798.02 is: "to make the laws of this state governing the use and disclosure of protected health information by covered entities consistent with, but generally not more stringent than, the HIPAA privacy rule for the purpose of eliminating barriers to the adoption and use of electronic health records and health information exchanges."

Policy:

1. Categories of Restricted Health Information Subject to This Policy

This policy applies to the exchange of records containing information pertaining to one of the following categories.

1.1 Drug and Alcohol Information

Federal law requires any disclosure of drug and alcohol information by a federally assisted program to be pursuant to patient authorization that meets certain requirements and also is accompanied by a written warning that prohibits re-disclosure of the information.

LEGAL REFERENCE: 42 CFR Part 2

1.1.1 IMPORTANT CLARIFICATIONS:

Not all information about drug and alcohol abuse or treatment is subject to federal Part 2 regulations.

1.2 Psychotherapy Notes

Federal law restricts disclosure of psychotherapy notes recorded by a mental health provider documenting or analyzing the contents of a conversation during a private, group or family counseling session and *that are separate from the rest of the patient's medical record.*

LEGAL REFERENCE: 45 CFR 164.508(a)(2)

1.2.1 IMPORTANT CLARIFICATIONS

This category should not be confused with mental health records *which are* a part of the patient's health record such as progress notes. Psychotherapy notes are *not* a part of a patient's health record. An example of psychotherapy notes are "process notes" that capture the therapist's impressions about the patient and may contain details of psychotherapy conversations considered inappropriate for the medical record. By definition, any of the following are also not considered psychotherapy notes: 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.

1.3. Services for Which Unemancipated Minors Have a Right to Control Disclosure

Under Ohio law, unemancipated minors under the age of 18 or those who are mentally or physically disabled and under 21 years of age may have the right to control disclosure of certain treatment information without the consent of their parent or legal guardian.

LEGAL REFERENCE: 45 CFR 164.502(g)(3) and ORC 3798.07

1.3.1 Examples of services to which a minor may consent without parental consent

Per state and federal law include:

a) Test results for HIV or sexually transmitted diseases;

b) The first six outpatient visits for mental health treatment; and

c) Blood donations through a non-profit organization.

Participants must ensure they have obtained the minor's consent to share information for services to which the minor had the sole right to consent for treatment and disclosure.

1.4 Services Paid in Full by Patient and Restricted From Disclosure to Health Plan/Payer

Under the HITECH Act, patients may request a Participant to restrict the disclosure of information regarding a health care item or service paid out-of-pocket in full by the patient to an insurance company, group health plan or other third party payer.

LEGAL REFERENCE: 42 USC 17935

1.4.1 IMPORTANT CLARIFICATIONS:

If a patient requests a Participant to restrict disclosure to their insurance company, the Participant can still share the information via directed exchange with Health Care Providers for treatment purposes.

1.5 Information Delivered to Ohio Department of Health for Public Health Reporting Purposes

Information delivered to the Ohio Department of Health ("ODH") for public health reporting purposes will be delivered through CliniSync using a separate dedicated interface to ODH.

LEGAL REFERENCE: n/a

1.5.1 IMPORTANT CLARIFICATIONS:

Since ODH makes public health reports available through its systems, CliniSync does not intend to duplicate this data in a patient's community health record at this time. Until further decisions are made and related agreements are in place, this information will not be accessible through the patient's CliniSync community health record. *Other pertinent legal references pertaining to these categories are included in Table 1 of this policy*.

2. General Participant Responsibility for Exchange of Restricted Health Information Exchange

Categories of restricted health information identified in this policy will not be accessible for query through the CliniSync HIE. Participants shall be responsible for ensuring that they do not submit restricted health information for query-based HIE, as described in Section 4. This does not preclude behavioral health participants or others from using query-based HIE to obtain other information (not restricted health information) about a patient they may be treating.

As described in Section 3, restricted health information may be transmitted using Direct Exchange Services, and then only after appropriate consent is obtained to comply with state and federal law.

Any disclosure of restricted health information through CliniSync Direct Exchange Services must be conducted in compliance with state or federal laws. Per CliniSync's Participant Agreement, compliance with state and federal laws for patient confidentiality, privacy, security and permitted and prohibited uses of data are the responsibility of the Participant.

a) Participants must evaluate and apply CliniSync policy within the context of their organization's environment and privacy policies. There may be instances where an organization's privacy policy is more restrictive (e.g., policies regarding information about VIPs).

b) Participants should be aware that clinical information accessible through the CliniSync HIE may not be complete if the sending Participant's privacy policies, state or federal law preclude making the information available to other Participants.

c) Any Participant that knowingly receives unauthorized restricted health information must follow CliniSync's Violation/Breach of CliniSync Policies or Participant Agreement. For these reasons, it is strongly recommended that this policy and any decisions made as to its use or applicability to your organization be shared with your organization's Privacy Officer.

3. Direct Exchange of Restricted Health information

Participants, including but not limited to ambulatory providers, may be behavioral health agencies, primary care physicians, specialists, nurse practitioners, clinics, hospital outpatient clinics and any other health professional or entity that provides outpatient care, that use Direct Exchange Services may be permitted to exchange restricted health information through those Direct Exchange Services.

Except for psychotherapy notes, all restricted health information categories identified in this policy may be exchanged among Participants using Directed Exchange if the Participant has obtained the appropriate consent as described in Section 1 above.

To facilitate compliance with state and federal laws that dictate more stringent patient consent and disclosure requirements, The Partnership strongly recommends the use of standard procedures approved by an organizations legal representative when exchanging information among Participants, who routinely treat minors over the age of 14 and/or information subject to Part 2 regulations. CliniSync provides educational materials with templates that can also be used, however Participants are responsible for determining whether/how these laws apply to them. Any questions participants have should be directed to their legal counsel.

4. Participant Responsibility for Excluding Restricted Health Information from HIE

Participants who provide data, including but not limited to lab results, transcribed reports, ADT and other clinical or administrative transactions for automated delivery through CliniSync to affiliated Health Care Providers are subject to requirements for handling restricted health information that may be contained in these transactions. All Participants contributing data for query -based HIE must either exclude, electronically tag or segregate data for restricted routing through CliniSync if it falls into a restricted category. Excluded, electronically tagged or segregated data will prevent the information from being accessible through a query of the patient's Community Health Record.

Participants who are data contributors are solely responsible for excluding, electronically tagging or segregating restricted information to comply with the laws governing this information. Since the method for electronically tagging restricted information may vary depending upon the capability of the Participant, the tagging method will be determined during the Participant's implementation cycle. If a Participant is unable to electronically tag restricted information, they must exclude it.

a) An exception to this policy is automated delivery of information pertaining to services to which an unemancipated minor has the right to control disclosure without the consent of a parent or legal guardian. This information will not need to be excluded, electronically tagged or segregated for restricted routing through CliniSync. Rather, patients over the age of 14 will be given the choice to explicitly opt-out of the HIE. If

the minor chooses to explicitly opt-out, none of their data will be available for query as described in Patient Consent Policy (D).

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Participant Obligations Under the Data Use and Reciprocal Support Agreement
Date of Board Approval: October 25, 2013
Applicable Services Direct Exchange Services and HIE Services

M. Participant Obligations Under the Data Use and Reciprocal Support Agreement Policy

Background:

This policy outlines and explains the requirements of the Data Use and Reciprocal Support Agreement (DURSA) directly applicable to The Partnership and its Participating Organizations. The DURSA is a legal, multi-party trust agreement entered into by The Partnership with other entities, organizations and Federal agencies that desire to engage in electronic health information exchange with The Partnership and its Participating Organizations. The DURSA sets forth a set of national standards, services and policies developed in coordination with Office of the National Coordinator for Health IT in the U.S. Department of Health and Human Services.

Policy:

1. Definitions.

For purposes of this policy, the following definitions shall apply. These definitions are intended to be the same as those set forth in Section 1 of the DURSA, and the definitions in Section 1 of the DURSA shall control in the event any difference exists, including differences due to future revisions of the DURSA. Further, any term used in this Policy that is not defined below but is defined in the DURSA shall have the meaning as provided in the DURSA.

Applicable Law shall mean all applicable statutes and regulations of Ohio, as well as all applicable Federal statutes, regulations, standards and policy requirements.

Authorization shall have the meaning and include the requirements set forth at 45 CFR § 164.508 of the HIPAA Regulations and include any similar but additional requirements under Applicable Law.

Breach shall mean the unauthorized acquisition, access, disclosure, or use of Message Content while Transacting such Message Content pursuant to this Agreement. The term ‘‘Breach’’ does not include the following:

1. any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Participating Organization if:

    a. such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participating Organization; and
    b. such Message Content is not further acquired, accessed, disclosed or used by such employee or individual; or
2. any acquisition, access, disclosure or use of information contained in or available through the Participating Organization’s system where such acquisition, access, disclosure or use was not directly related to Transacting Message Content.

Health Care Operations shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

Message shall mean an electronic transmission of Message Content Transacted between DURSA participants using the Specifications. Messages are intended to include all types of electronic transactions as specified in the Performance and Service Specifications, including the data or records transmitted with those transactions.

Message Content shall mean that information contained within a Message or accompanying a Message using the Specifications. This information includes, but is not limited to, Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonymized data, metadata, digital credentials, and schema.

Participating Organization shall have the same meaning as set forth in Policy A and shall mean for the purposes of this Policy “Participant User” as that term is defined in the DURSA. That is, each Participating Organization is a “Participant User” for purposes of The Partnership’s compliance with the DURSA.

Performance and Service Specifications shall mean the Validation Plan and the Specifications, as well as any implementation guidance, migration plans and other technical materials and resources approved by the DURSA Coordinating Committee.

Permitted Purpose shall mean one of the following reasons for which Participating Organizations may legitimately Transact Message Content:

1. Treatment of the individual who is the subject of the Message.
2. Payment activities of the Participating Organization for the individual who is the subject of the Message which includes, but is not limited to, Transacting Message Content in response to or to support a claim for reimbursement submitted by a Participating Organization to a Health Plan.
3. Health Care Operations of either:
    a. the Submitter if the Submitter is a Covered Entity;
    b. a Covered Entity if the Submitter is Transacting Message Content on behalf of such Covered Entity; or
    c. the Recipient if (i) the Recipient is a health care provider who has an established Treatment relationship with the individual who is the subject of the Message or the Recipient is Transacting Message Content on behalf of such health care provider; and (ii) the purpose of the Transaction is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance of such health care provider.
4. Public health activities and reporting as permitted by Applicable Law, including the HIPAA Regulations at 45 C.F.R. § 164.512(b) or 164.514(e).
5. 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, provided that the purpose is not otherwise described in subsections 1-4 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.
6. Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations.

Recipient shall mean the Participating Organization(s) that receives Message Content through a Message from a Submitter for a Permitted Purpose. For purposes of illustration only, Recipients include, but are not limited to, Participating Organizations who receive queries, responses, subscriptions, publications or unsolicited Messages.

Specifications shall mean the specifications adopted by the DURSA Coordinating Committee to prescribe the data content, technical, and security requirements to enable the DURSA participants to Transact Message Content. Specifications may include, but are not limited to, specific network standards, services and policies.

Submitter shall mean the Participating Organization(s) who submits Message Content through a Message to a Recipient for a Permitted Purpose. For purposes of illustration only, Submitters include, but are not limited to, Participating Organizations who push Messages with Message Content, send Messages seeking Message Content, send Messages in response to a request, send subscription Messages, or publish Messages with Message Content in response to subscription Messages.

Transact shall mean to send, request, receive, assert, respond to, submit, route, subscribe to, or publish Message Content using the Performance and Service Specifications.

Treatment shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.

Validation Plan shall mean the framework for Testing and demonstrations for parties seeking to become DURSA participants.

2. General Obligations.

Each Participating Organization shall:

a. Comply with all Applicable Law.
b. Reasonably cooperate with The Partnership on issues related to the DURSA.
c. Transact Message Content only for a Permitted Purpose.
d. Use Message Content received from other Participating Organizations in accordance with the terms and conditions of the DURSA.
e. As soon as reasonably practicable after determining that a Breach occurred, report such Breach to The Partnership in accordance with Policy K. Sanctions for Violation/Breach of Permitted Use.
f. Refrain from disclosing to any other person any passwords or other security measures issued to the Participating Organization.

3. Permitted Purpose.

Participating Organizations shall only Transact Message Content for a Permitted Purpose as defined in this Policy. Each Participating Organization shall Transact Message Content only in accordance with the terms and conditions of this Policy, including without limitation those governing the use, confidentiality, privacy, and security of Message Content. Each Participating Organization shall discipline appropriately any of its Authorized Users who fail to act in accordance with the terms and conditions of this Policy relating to the privacy and security of Message Content. Additional restrictions may apply on the permissible disclosures in other Policies and those restrictions must be met even if the disclosure would be allowed as a Permitted Purpose under this Policy.

4. Minimum Requirement for Participating Organizations that request Message Content for Treatment.

All Participating Organizations that request Message Content for Treatment shall have a corresponding reciprocal duty to respond to Messages that request Message Content for Treatment. A Participating Organization shall fulfill its duty to respond by either (i) responding to the Message with the requested Message Content or (ii) responding with a standardized response that indicates the Message Content is not available or cannot be exchanged. All responses to Messages shall comply with the Performance and Service Specifications, the DURSA, and Applicable Law. Participating Organizations may Transact Message Content for a Permitted Purpose other than Treatment.

Each Participating Organization that requests Message Content for Treatment shall Transact Message Content for Treatment in accordance with the Performance and Service Specifications and the DURSA.

5. Specific Duties of a Participating Organization When Submitting a Message.

Whenever a Participating Organization acts as a Submitter by submitting a Message to another DURSA participant, the Submitter shall be responsible for:

a. Submitting each Message in compliance with Applicable Law and this Policy including, but not limited to, representing that the Message is:
    i. For a Permitted Purpose.
    ii. Submitted by a Submitter who has the requisite authority to make such a Submission.
    iii. Supported by appropriate legal authority for Transacting the Message Content including, but not limited to, any consent or Authorization, if required by Applicable Law.
    iv. Submitted to the intended Recipient.
b. Representing that assertions or statements related to the submitted Message are true and accurate.
c. Submitting a copy of the Authorization, if the Submitter is requesting Message Content from another DURSA participant based on a use or disclosure pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative as described in 45 C.F.R. § 164.502(g) of the HIPAA Regulations

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: HISP Provider Directory
Date of OHIP Approval: 10/16/2014
Applicable Services: Direct Exchange Services

N. HISP Provider Directory

Background: The Partnership serves as a Health Information Service Provider ("HISP") providing direct messaging services to Participating Organizations. Some Participating Organizations use third-party HISPs to provide such direct messaging services. This policy sets forth guidelines for the provisioning and exchange of direct addresses.

Policy:

I. PROVISIONING OF DIRECT ADRESSES

a. HISPs provide recipient users with specific direct email addresses for each health care provider to use for direct messaging (a "Direct Address").

b. When providing services as a HISP, the Partnership creates Direct Addresses for the Participating Organizations' health care providers.

c. Participating Organizations using the Partnership as a HISP may only create Direct Addresses for health care providers of the Participating Organization or any of its affiliated entities listed in Exhibit B of the Participant Agreement.

d. Direct Addresses provided by the Partnership may be exchanged by the Partnership with third party HISPs and other Participating Organizations.

II. DIRECTORY EXCHANGE

a. Directory Information. Directory Information means the information listed in Exhibit 1 to this policy for each Direct Address.

b. Exchange of Directory Information. Subject to Sections II.c and II.d below, the Partnership and each Participating Organization shall provide to the other for inclusion and use in the healthcare provider directory of the other party the Directory Information relating to healthcare providers for whom they have provisioned Direct Addresses and Directory Information from third party HISPs who have authorized the exchange of such information by written agreement.

c. Permitted Uses; Ownership. Each Party receiving Directory Information (the "Receiving Party") provided by the other party (the "Disclosing Party") may store and use, in perpetuity, such Directory Information solely to (i) support the clinical messaging and related services provided by the Receiving Party solely to those healthcare providers whose Direct messaging services are directly administered by the Receiving Party or its HISP, and (ii) permit third party HISPs to search the Directory Information by healthcare provider name (the "Search Capability"). The Disclosing Party grants no license(s) to the Receiving Party with respect to the Disclosing Party's Directory Information and the Disclosing Party shall retain full and exclusive right, title, and interest to such Directory Information.

d. Prohibited Uses. The Receiving Party may not use the Disclosing Party's Directory Information for any purpose not set forth in Section II. c without the express written permission of the Disclosing Party, including but not limited to: (i) providing to any third party HISP, or permitting a third party HISP to acquire or create, a copy of the Disclosing Party's Directory Information or any portion thereof; (ii) otherwise selling, disclosing, or making available the Disclosing Party's Directory Information to any third party; or (iii) for direct marketing, database marketing, telemarketing, marketing analysis, service bureau, or research purposes.

e. Commercial Messaging Rules.
   1. General Limitation. In addition to the restrictions set forth above, neither Party may use the Directory Information in conjunction with any means, program, or device, or permit any other person to use the Directory Information in conjunction with any means, program, or device, including, but not limited to, advertising, instant messaging, and pop-up ads, to solicit business or to influence or attempt to influence for commercial purposes (through economic incentives or otherwise) any diagnostic or treatment-related decision of a health care provider. The bona fide professional recommendation of a health care provider offered to another health care provider regarding the treatment or diagnosis of a shared patient is not intended to be prohibited by this provision; however, the Disclosing Party shall have sole discretion to determine the bona fide non-commercial and clinical nature of all messages.
   2. Exceptions to General Limitation. Notwithstanding the above Section II.e.1, either Party may (and may permit authorized users to): (A) use the Directory Information to communicate information regarding a patient's health care coverage, including patient lowest cost options, on/off tier, prior authorization, step therapy, coverage status, and co-pay information; and/or (B) deliver or have delivered to health care providers clinical alerts that are sourced from payers and/or are attributed to generally recognized and reputable sources providing clinical information, even if, in the event of either (A) or (B), such information influences the health care provider's treatment decisions.

f. Format. The Parties shall exchange Directory Information in the implementation guide format attached in Exhibit 1 to this policy at a frequency agreed to by both parties.

Exhibit 1

Directory Information

Contract	Field
C	HISP Provider Identifier (SPI). Only for records containing the Direct Address.
R	Direct Address (aka. Network Address)
C	NPI
O	Prefix Name
R	First Name
O	Middle Name
R	Last Name
O	Suffix Name
O	Specialty
O	Specialty Code
O	Organization Name / Location Name (Typically Clinic)
R	Address Line1
C	Address Line2
R	City
R	State

C – Conditional (if known, please provide)
R – Required
O – Optional

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Data Deletion
Date of Board Approval: June 12, 2015
Applicable Services: Direct Exchange Services and HIE Services

O. Data Correction and Deletion Policy

Background:

The prevention of unauthorized changes or deletion of the Protected Health Information of Participating Organizations is a priority of the Partnership. Scenarios may arise that require data sent by a Participating Organization to CliniSync to be corrected or deleted. The following policy will govern if and when this can occur.

Policy:

1. Correction of Data

It is the preference of the Partnership to avoid the deletion of data and instead to correct data wherever possible.

1.1 Circumstances that Qualify for Data Correction

The following circumstances qualify as a reason for a Participating Organization to pursue the correction of data from the CliniSync HIE.

a) Demographic information for a patient is incorrect within a result or report
b) Clinical information for a patient is incorrect within a result or report
c) Data that is Protected Health Information has been amended by a Participating Organization under the HIPAA Privacy Regulations

1.2 Method of Data Correction

If a Participating Organization chooses to correct data, the preferred method of correction is to send the correct data through the existing interface between the Participating Organization and CliniSync. The corrected data is appended to the individual's patient record within the HIE, where a record will always exist of the original data but will not be viewable to a CliniSync user. This process is managed by the Participating Organization. The Partnership staff can and will offer assistance in this process if requested by the Participating Organization.

2. Deletion of Data

Situations may arise that require the complete deletion of data or a set of data that was sent to the CliniSync HIE. Data that has been accessed by any CliniSync user will not be eligible for data deletion and will instead need to be corrected as described in Section 1.2. The reason for this is that if data has been viewed by a clinician during the treatment of a patient that data must be retained for future reference. Furthermore, data will not be considered for deletion if it is possible for the Participating Organization to correct the data as described in Section 1.2.

2.1 Circumstances that Qualify for Data Deletion

Either of the following circumstances below qualify as reasons for a Participating Organization to pursue the deletion of data from the CliniSync HIE.

a) A Participating Organization leaves the CliniSync HIE. This may take place if the Participating Organization goes out of business, the Participating Organization chooses to cease participation in CliniSync due to an inability to comply with CliniSync policies, or if the Participating Organization is purchased by another organization who does not wish to participate in the CliniSync HIE.
b) A Participating Organization erroneously sends CliniSync incorrect Protected Health Information in Production and on investigation by CliniSync staff, no users have accessed the data and the contributing organization has no way to remediate the issue through existing interface workflows.

2.2 Method of Data Deletion

If one of the above qualifying circumstances exists, the following must occur prior to deletion of the Participating Organization's data.

a) The Participating Organization must contact the CliniSync Privacy or Security officer immediately.
b) The Participating Organization must explain the situation that warrants the deletion of data from the CliniSync HIE in writing. A record of this explanation will be maintained by CliniSync in accordance with HIPAA data retention compliance.
c) The request will be reviewed by the CliniSync Privacy Officer, CliniSync Security Officer and Senior Management.
d) If deletion is approved, the Participating Organization will work with Partnership staff and the Partnership's technology vendor to delete the data.

3. Records of Data Deletion

If data is deleted permanently from the CliniSync HIE, there will be no auditable record that such data was ever sent to the HIE. For this reason, it is imperative that the deletion of the data is well documented. A Participating Organization must send the Partnership a copy of the incorrect data and the correct data along with a thorough explanation of the circumstance that led to the

decision to permanently delete the errant data prior to the actual deletion of data. All documentation will be kept and stored by the Partnership in accordance with HIPAA data retention compliance.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC POLICY
Subject: Notification Services Policy
Date of Board Approval: August 11, 2017
Applicable Services: Direct Exchange Services

P. Notification Services Policy

Background:

Providers of care and others with care responsibility are increasingly being held accountable for improved and timely post-discharge care coordination and reduced readmission rates. To assist, CliniSync provides a Participating Organization a service to receive real time notifications of events such as hospital inpatient admission, an emergency room encounter or an outpatient encounter. The hospital events that trigger the real-time electronic notifications can be technically described as Health Level Seven (HL7) Admission, Discharge and Transfer (ADT) messages from hospital information systems. These alerts can be used to help better coordinate a patient's care. This policy provides data governance policies specific to CliniSync Notification Services.

Definitions Specific to this Policy

"**Subscribing Participating Organization**" shall mean an organization who has contracted with the Partnership for CliniSync Notification Services and has met all requirements as described in section 2 of this policy.

"**Notification Information**" shall mean information available from CliniSync Notification Services as defined in section 1 of this policy.

Policy:

1. Information available from CliniSync Notification Services

The only information available via CliniSync Notification Services is HL7 ADT information from hospitals who have an existing Participant Agreement with the Partnership. This information is further limited as described in section1.1.

1.1 The information available from CliniSync Notification Services is restricted to only the data listed in this section.

a) Patient Demographic Information
b) Patient Status Information

2. Requirements for Participating Organizations who subscribe to CliniSync Notification Services

2.1 The Subscribing Participating Organization must sign a contract addendum to the CliniSync Participant Agreement to use the service. This contract includes a description of the permitted uses of the data delivered as part of CliniSync Notification Services and described in Section 1.1.

2.2 The Subscribing Participating Organization must submit and maintain an active patient list for whom they want to receive notifications to the Partnership via an approved process prescribed by the Partnership. The active patient list must only include "Active Patients" as described in section 3.1.

3. Patient List Criteria

Prior to receiving Notification Information from CliniSync participating hospitals, a Participating Organization must submit an active patient list to the Partnership. This active patient list should only include "Active Patients" as defined in section 3.1. The Participating Organization must regularly update their active patient list and notify the Partnership of changes to the active patient list via a process prescribed by the Partnership.

3.1 Active Patient Criteria

Patients included on the Participating Organization's active patient panel must meet all following criteria.

a) Patient has an existing treatment relationship with the Participating Organization.
b) Patient has had a clinical encounter with the Participating Organization within the past 24 months or is attributed to the organization.
c) Patient has actively enrolled in a care management program that permits data sharing and has the ability to disenroll or otherwise opt out of the care management program.

OHIO HEALTH INFORMATION PARTNERSHIP CLINISYNC HEALTH PLAN POLICY
Subject: Notification and Clinical Exchange Services for Organizations Managing Populations
Date of Board Approval: August 11, 2017
Applicable Services: Direct Exchange Services

Q. Notification and Clinical Exchange Services for Organizations Managing Populations

Background:

As our stakeholders assume increased responsibilities for **value-based, patient-centric care**, many have approached CliniSync to support better care coordination and quality improvement for populations they serve. These stakeholders share a common need to exchange event notifications, clinical data and claims or other relevant data more effectively to successfully participate in emerging performance-based or shared-risk payment models. They include not only Health Plans, but provider-driven Accountable Care Organizations (ACO), Clinical Integrated Networks, Chronic Care Management organizations and others that share contractual responsibility for the quality, cost or overall care of a population. All are driven by a common need to advance care coordination, reduce gaps in care, and track and improve quality measures.

This policy provides governance specific to data that will be made available to organizations managing populations. Data will be limited to specific HIPAA-permitted uses as described in this policy to ensure stakeholder trust.

Definitions Specific to this Policy:

"Population Health Service Organization" (PHSO) shall mean a Covered Entity or Business Associate of a Covered Entity that is contractually responsible for the quality, cost or overall care of a population, including Medicare beneficiaries, third party beneficiaries or beneficiaries participating in an alternative payment model program such as an accountable care organization. Health care providers participating in the PHSO are "**PHSO Members**".

"Health Plan" shall mean an individual or group plan that provides, or pays the cost of, medical care, and that is a covered entity as defined under HIPAA.

"Active Population List" shall include any member currently enrolled in a health plan or with an active treatment or other patient relationship with PHSO or a PHSO Member.

General Requirements for Organizations Managing Populations

- The organization must be a Population Health Service Organization or a Health Plan.
- The organization must have an existing Participant Agreement with the Partnership that includes HIE services necessary to receive data for a population.
- The organization must have an active relationship with the patient for whom it receives data.
- The organization must have a contractual responsibility for the HIPAA-permitted use. The data available must align with the contracted HIPAA permitted use.
- The organization must provide and maintain an Active Population List via an approved process prescribed by The Partnership.
- The organization accepts responsibility for the accuracy and timeliness of the Active Population List.

Requirements for Specific HIPAA-Permitted Uses

1. NOTIFICATIONS

   Permitted Use Service

   CliniSync provides organizations a service to receive real time notifications of events such as hospital inpatient admission, an emergency room encounter or an outpatient encounter for their population. The hospital events that trigger the real-time electronic notifications can be technically described as Health Level Seven (HL7) Admission, Discharge and Transfer (ADT) messages from hospital information systems. These alerts can be used to help better coordinate a patient's care.

   Permitted Use Population Restrictions

   Organizations managing populations may receive notifications for their Active Population List.

   Permitted Use Data Available

   The limited set of clinical and other contributed data available for this use will be documented as a CliniSync procedure, reviewed and approved by the Executive Committee annually or more frequently as needed.

2. CASE MANAGEMENT AND CARE COORDINATION

Permitted Use Service

CliniSync provides organizations a service to receive a limited set of clinical and other contributed data for case management and care coordination as permitted for Health Care Operations purposes and as further defined (45 CFR 164.501).

Permitted Use Population Restrictions

Organizations may receive data for their Active Population List identified as emerging, high or intensive risk such a population that is part of care management programs within their population and for whom the organization is contributing reciprocal data to the HIE. CliniSync and organization must approve how to identify "emerging, high or intensive risk" patients prior to the organization receiving data.

Permitted Use Data Available

The limited set of clinical and other contributed data available for this use will be documented as a CliniSync procedure, reviewed and approved by the Executive Committee annually or more frequently as needed.

3. QUALITY ASSESSMENT AND IMPROVEMENT

Permitted Use Service

CliniSync provides organizations a service to receive a limited set of clinical and other contributed data for quality assessment and improvement as permitted for Health Care Operations purposes and as further defined (45 CFR 164.501).

Permitted Use Population Restrictions

Organizations may receive data for their Active Population List for whom the organization has contributed reciprocal data.

Permitted Use Data Available

The limited set of clinical and other contributed data available for this use will be documented as a CliniSync procedure, reviewed and approved by the Executive Committee annually or more frequently as needed.