



HEALTH INFORMATION AND DATA SHARING Fact Sheet

Legal Frameworks to Improve Health Equity Through Community Information Exchanges


The exchange of timely health and social services information is vital to advancing the health and well-being of all members of our communities. The Network for Public Health Law recently collaborated with the Illinois Public Health Institute to provide legal technical assistance and support development of the [Chicago Regionwide CIE](#), a Community Information Exchange (CIE™), that will serve Chicago and Cook County, Illinois. Network attorneys reviewed just under twenty CIEs, social health information exchanges (S-HIEs), and other CIE-like initiatives that are in differing stages of development or implementation. This resource examines common features of legal frameworks developed to facilitate the flow of information in CIEs around the country.

Community Information Exchanges

A CIE™ is a community governed network of health and social service providers that can facilitate data sharing among healthcare, social services, and community-based organizations to facilitate more holistic and coordinated care, and advance public health. CIEs have been created in several parts of the country, offering the opportunity to share an individual's data beyond the traditional health care or social services setting, to providers and community-based organizations (CBOs) that address health care, housing, social services, and a host of additional supports. Common features of CIEs include:

- identified organizational participants, including health care providers and social services providers;
- informed consent from the individuals whose data will be shared;
- longitudinal records;
- integrated technology platforms to allow for exchange of data;
- backbone entities managing the CIE™; and
- strong data governance to ensure the quality, accuracy, and responsible and ethical use of data.

Access to the timely and accurate health and social services information of individuals reduces the likelihood that key health history and other information will be overlooked, provides for more holistic care, and improves coordination of, and access to, services. However, for a number of reasons, health and social services



information is often not available to each service provider with whom individuals interact. Referrals and services are often siloed, and health and social services providers only have a partial snapshot of the individual client's needs and services. As a result, clients may not have access to needed services and support.

CIEs provide a legal and ethical structure to share this information with an individual's consent, to ensure these individuals are better served by providers. Responsible and consented sharing of individuals' information also reduces the likelihood that individuals with complex needs will have to repeat their health and social services history, potentially retraumatizing the individual, to each new service provider with whom they engage. With their person-centered approach and explicit recognition that health outcomes are largely determined by social drivers of health, CIEs can move the needle on health equity and well-being for people and communities facing systemic barriers.

Systems and structures perpetuate grossly uneven access to resources, and people of color [disproportionately experience](#) health-related social needs driven by [structural racism](#) and other systems of oppression. CIEs have the potential to illuminate an individual's needs and ensure those most in need, such as those subject to the on-going effects of racism, access services and maintain their dignity and agency in the process.

CIEs in Practice: A Case Study on Health, Incarceration, and Homelessness


To understand how CIEs can function in practice, consider the following hypothetical on disrupting health-harming cycles of incarceration and homelessness:

The staff of a city health department noticed that a high proportion of incarcerated people in the city jail were repeatedly brought in for the same misdemeanors and minor infractions. Upon closer examination, the staff noticed this same population had a very high rate of behavioral health issues, either a mental health condition or substance use disorder (or both), and were often unhoused. Once released, these individuals often had no home to return to or way to access mental health care or SUD treatment services.

Even if they received a referral for services prior to leaving the jail, there was no way for a health care provider or social services provider to know about the referral or see the person's information, such as medications or social services they had previously accessed. This meant that a person returning to their communities lacked access to care in the weeks following release, when the risk of overdose and suicide attempts is significantly heightened. And if that person returned to jail, the jail health services often had no way of knowing what the person's behavioral health needs (such as medications) were.

The city health department, community members, and other partners could collaborate to establish a CIE™ with a focus on addressing the needs of unhoused individuals with behavioral health issues cycling in and out of the city jail. A consent-driven system for securely and responsibly sharing individual data with providers across sectors could help to disrupt the punitive cycle and promote access to services that meet individuals' with the goal of improving the likelihood that they will stabilize over time. Specifically, a CIE™ could aim to facilitate:

- sharing of data on an incarcerated individual's health and social needs and treatment plans with providers (e.g., behavioral health providers, homeless services agencies, CBOs) to ensure care provided is responsive, informed, and person-centered;
- closed-loop referrals to strengthen linkages and avoid lapses in care; and

- 
- development of a longitudinal record to assist providers in understanding service needs and eligibility over time.

The CIE™ would be community-driven, centering the voices of those directly impacted (in this case, individuals who are or formally were incarcerated and unhoused). And it would operate under a legal and governance framework that safeguards individual privacy, protects against harmful uses of data, and ensures compliance with legal requirements.

Legal Frameworks to Facilitate Data Exchange Through a CIE™

Exchange of individually identifiable health information presents significant risks to the privacy of the individual—risks that must be managed carefully. The legal challenges relating to exchanging individual-level data are further complicated when sharing data across sectors, each with its own legal landscape. Some common components of legal frameworks to facilitate data exchange through a CIE™ are discussed below.

Robust Consent

A robust informed consent model, with the individual explicitly authorizing the exchange of their information within the CIE™, is commonly the legal basis that permits data exchange through a CIE™. It would be difficult, if not impossible, to share sensitive, individually identifiable information with all the partners in a CIE™ without the individual's consent. An opt-in consent model—where individuals are assumed not to have consented until they actively provide written or electronic consent—prioritizes individual autonomy, allowing individuals to control who can access their personal data.


Participant Agreements

CIEs may be built around several agreements designed to ensure compliance with relevant laws and establish a clear data governance structure. These agreements may include participation agreements, business associate agreements, data use agreements, and other agreements. As is true of all elements of a CIE™ legal framework, these agreements vary in form and content and should be structured to align with the flow of data within the specific CIE™. For example, a CIE™ could involve data flows between a CIE™ backbone entity, hospitals and other health care providers, shelters, and social service agencies. These participants, together with the types of data, direction of data, sensitivity of data, intended uses, applicable law, and other considerations will dictate which agreements are advisable for the data exchange project.

Participation Agreements

A participation agreement involving all participants can ensure that all stakeholders operate within a well-defined, secure, and compliant data-sharing framework. Regardless of the form of the agreement, the challenge lies in establishing terms acceptable to all parties.

While there is no single template for a participation agreement, it should clearly outline responsibilities related to participation in, and use of, the CIE™. For example, the agreement may spell out the purpose of the data exchange, permitted uses of data by the CIE™ and participants, require that participants obtain necessary consents and ensure data is shared only as permitted by the agreement. The agreement may also state whether parties may engage third parties for specific roles.



The participation agreement may define general rights and obligations of the CIE™ participants, including:

- scope of participation,
 - types of data exchanged,
 - restrictions on certain categories of data (e.g., HIV, behavioral health, domestic violence),
 - permitted uses of data received by a participant (e.g., allowed for shelter-based care and care coordination, but prohibited for marketing or monetization),
 - specific data retention policies,
 - acknowledgment of system components, such as application programming interfaces (APIs), master patient indexes (MPIs), and consent catalog engines,
 - actions to be taken in the event of a data breach, and
 - information security requirements, ensuring all parties implement safeguards that protect the confidentiality, integrity, and availability of data.
-


Business Associate Agreements

Data flows within a CIE™ structure may dictate the need for one or more business associate agreements (BAAs) in certain circumstances. Business associate agreements ensure that third parties with access to protected health information (PHI) of a Health Insurance Portability and Accountability Act (HIPAA) covered entity properly safeguard the PHI and use it only as permitted. HIPAA covered entities must obtain “satisfactory assurances” that a business associate will protect PHI, typically in the form of a BAA.

Business associates fall into two categories:

1. entities handling PHI on behalf of a covered entity for regulated activities such as claims processing, data analysis, or utilization review, and
2. certain service providers (e.g., legal, accounting, consulting, or financial services) that require access to PHI of the covered entity to perform their service.

According to Section 17938 of the HITECH Act, any organization that transmits Protected Health Information (PHI) to a covered entity and requires regular access to PHI, such as a health information exchange organization, is considered a business associate of the covered entity. “Entities that manage the exchange of protected health information through a network, including providing record locator services and performing various oversight and governance functions for electronic health information exchange, have more than “random” access to protected health information and thus, would fall within the definition of “business associate.””¹



Although CIEs are not referenced in the HIPAA Privacy Rule, the role of any given CIE™ may be similar to that of Health Information Organizations (HIOs), however, such determination requires legal analysis. While the Department of Health and Human Services (HHS) has not formally defined an HIO, a CIE™ that facilitates and manages information exchange between covered entities, social service providers, and other stakeholders may function in a comparable way to HIO—if not as an actual HIO. However, HHS does not appear to discuss CIEs in any of its guidance. Identifying any entity as a business associate is always a case-by-case, fact-specific determination that requires careful analysis, preferably with the assistance of legal counsel.

Data Use Agreements


A data use agreement (DUA) establishes the terms and conditions for handling data. This agreement ensures that parties participate in data exchange while adhering to strict security, privacy, and compliance standards. A data use agreement may be of particular value in the case of non-HIPAA-covered-entity participants (such as shelters, HMIS lead agencies, and 211-service providers) that exchange data but are not required under HIPAA to have a business associate agreement. Whether or not to use a DUA, in what instances to use a DUA, and from whom to require DUAs is another decision that requires careful analysis.

The DUA outlines how data is collected, stored, used, and disclosed. Components of a data use agreement may include, for example:

- identifying the parties and the purpose for entering into the agreement (this section may also state the legal authority to enter into the agreement);
 - defining obligations, such as the CIE™ backbone entity's role in securely receiving, storing, and making data accessible or requiring participants to ensure necessary consents before sharing data;
 - detailing which data elements are to be exchanged, how data is transmitted (directly or through intermediaries), and how it is managed (or destroyed) upon agreement termination;
 - requiring an information security program to show the entity adequately manages data security to ensure the confidentiality, integrity, and availability of the data;
 - setting rules for third-party access, such as law enforcement requests and subpoena notifications, as well as limitations on secondary uses (e.g., research, public health); and
 - establishing that only the minimum necessary data should be shared for specific use cases.
-

Policies and Procedures

A CIE's policies and procedures—a key component of the legal framework—are intended to govern the CIE's operations. Policies and procedures help to ensure that a CIE's data sharing practices comply with legal



requirements. They further advance a CIE’s mission of promoting access to person-centered, holistic care, and protect against harmful uses and disclosures of data. In an equitable data sharing system, policies and procedures are driven by, and reflect the voices of, directly impacted communities whose data may be shared through the CIE™.

Policies and procedures may govern data collection, use, and disclosure, identifying what data is collected through the CIE™, the purposes for which it may be used and disclosed, and restrictions on use and disclosure, as well as any additional restrictions for particularly sensitive data (e.g., data on HIV, SUD, reproductive health care). Other areas that may be covered by policies and procedures include consent requirements, individual rights, data minimization, data access, data security, and data quality. The policies and procedures can additionally help to ensure that participating organizations act in accordance with the CIE’s mission through a selection policy that establishes a process and criteria for determining organizational participation in the CIE™.

Conclusion

Many parts of the country are developing or implementing CIEs. They have the potential to advance health equity by advancing whole-person care that works to address the underlying social drivers of health. As with any data sharing initiative, however, close attention must be paid to legal considerations. A strong legal framework, robust informed consent, appropriate agreements, policies and procedures and other elements may pave the way for a successful community information exchange.

This document was developed by Stephen Murphy, J.D., Director, Meghan Mead, J.D., Deputy Director, and Emma Kaeser, J.D., Staff Attorney, Network for Public Health Law—Mid-States Region. The Network promotes public health and health equity through non-partisan educational resources and technical assistance. These materials provided are provided solely for educational purposes and do not constitute legal advice. The Network’s provision of these materials does not create an attorney-client relationship with you or any other person and is subject to the [Network’s Disclaimer](#).

04/11/2025

SUPPORTER

Support for the Network provided by the Robert Wood Johnson Foundation. The views expressed in this document do not necessarily reflect the views of the Foundation.



Robert Wood Johnson Foundation

¹ Department of Health and Human Services (HHS), *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rule*, [78 Fed. Reg. 5566, 5571 \(Jan. 25, 2013\)](#).