Journal of Law, Medicine & Ethics (2026), **54**, S1, 54–61
doi:10.1017/jme.2026.10238

CAMBRIDGE UNIVERSITY PRESS

Symposium Articles

An Analysis of Legal Considerations for Sharing Data Through Community Information Exchanges (CIEs)

Stephen Murphy, Meghan Mead, and Emma Kaeser
The Network for Public Health Law, United States

Abstract

Amid growing interest in the integration of health and social care to improve outcomes, communities across the United States have explored development of Community Information Exchanges (CIEs). A CIE is a community governed infrastructure that enables critical health and social information to be responsibly shared among partner organizations in support of holistic coordination of care. The development and use of a CIE give rise to a host of legal and policy challenges. Use and disclosure of data through a CIE are governed by a patchwork of different legal requirements, at times distinct and at times overlapping. Development of a legal framework for a CIE requires attention to clearly articulated data flows, detailed use cases, strong legal agreements and policy considerations. CIEs typically rely on an individual's express consent to share their information, requiring careful evaluation of applicable laws and regulations and promotion of community trust and equity. And because many participants in a CIE are HIPAA covered entities, functions of the CIE must fit within HIPAA's regulatory framework. This article examines in depth two components of a sound legal framework—consent models and HIPAA compliance—identifying considerations and lessons learned to support lawful and ethical information sharing through a CIE.

Keywords: Data; Health Equity; Community; Consent; HIPAA

Introduction

A robust body of evidence demonstrates that health outcomes are shaped by social conditions, such as access to healthy food, housing, employment, and transportation.[1] Improving an individual's health may require ensuring that they receive necessary medical care but also, for example, that they have access to healthy food[2] and reliable transportation to travel to appointments and pick up medication.[3] Health and social care thus ideally reinforce each other to create conditions in which people can live healthy, thriving lives.[4] But health and social care are often fragmented; these systems, distinct from each other across numerous measures, have historically operated separately, failing to communicate and coordinate on a systematic basis.[5] Recognizing the potential of integrated cross-sector care, the health and social services fields are increasingly exploring opportunities to improve coordination of their efforts to serve people with health and health-related social needs.[6]

Amid this growing interest in the integration of health and social care, communities across the United States have explored development of Community Information Exchanges® (CIEs). CIEs are community-governed systems that facilitate data sharing among local health and social services providers and community-based organizations to promote holistic and coordinated care.[7] Similar initiatives go by other names, such as social health information exchanges.[8] By improving access to services that address social drivers of health, these initiatives can mitigate systemic barriers and resource disparities that harm the health of structurally marginalized communities. And, when they are built by the communities they serve, these initiatives foster trust and build power among those directly impacted, advancing equity in systems of health and social care.

While CIEs and similar initiatives have the potential to promote holistic, coordinated care for people with health and health-related social needs, their use poses challenges from a legal standpoint, as CIEs implicate a host of legal issues related to privacy law compliance, consent models, and agreement structures. Drawing from lessons learned developing a CIE legal framework, this article explores considerations and best practices for navigating these issues. It first provides further background, describing common goals and features of CIEs and expanding on the legal and policy challenges that CIEs entail. It subsequently addresses general considerations for development of a legal framework. Finally, it examines legal questions, considerations, and lessons learned related to two primary components of a CIE legal framework: consent models and compliance with the Health Insurance Portability and Accountability Act (HIPAA). These findings can support development of a legally sound framework for information sharing that advances health equity through a trusted, accountable, and community-driven system.

CIE Purpose and Common Features

CIEs aim to connect a wide range of providers and organizations that address health and health-related social needs. These may

Corresponding author: Stephen Murphy; Email: smurphy@networkforphl.org
Cite this article: S. Murphy, M. Mead, & E. Kaeser. "An Analysis of Legal Considerations for Sharing Data Through Community Information Exchanges (CIEs)," *Journal of Law, Medicine & Ethics*, **54**, S1 (2026): 54–61. https://doi.org/10.1017/jme.2026.10238

© The Author(s), 2026. Published by Cambridge University Press on behalf of American Society of Law, Medicine & Ethics.

https://doi.org/10.1017/jme.2026.10238 Published online by Cambridge University Press

include Federally Qualified Health Centers (FQHCs), hospitals, behavioral health services, health plans, housing and homeless services organizations, food pantries, transportation services, community centers, and disaster relief organizations.[9] As CIE participants, these parties can exchange information with each other about the individuals they serve, with the goal of advancing coordinated, wraparound services. CIEs also seek to reduce the burden on individuals navigating fragmented and complex systems of care.[10] Navigating such systems and having to repeatedly share one's own personal information with countless providers can be frustrating, even retraumatizing for those with histories of trauma.[11]

Access to resources is grossly uneven, with people of color, people with low or no income, people with disabilities, and other systemically marginalized groups disproportionately experiencing health-related social needs driven by structural racism and other forms of oppression.[12] CIEs and similar initiatives can work to advance health equity by ensuring that those who are systemically underserved have access to needed services and support, fostering autonomy and dignity in the process.

Although CIEs vary in many respects, they typically involve certain key features and functionalities. Most CIEs have a backbone entity, which could be a public or private organization, that manages the CIE.[13] CIEs also aim to be community driven; thus another common feature is decision-making systems that vest power in impacted communities. Such systems may take the form of committees or workgroups of people with lived experience navigating systems of health and social care who inform and make decisions related to the CIE's operations.[14] CIEs also commonly involve an agreement structure formalizing the relationships among the participants and setting forth their responsibilities.[15] And CIEs generally use and disclose data only pursuant to individual consent.[16]

A robust data governance framework is also typical of CIEs.[17] This framework encompasses the terms shaping data exchange, use, and stewardship set forth in policies, procedures, practices, and agreements. Strong data governance that is built by impacted communities ensures that data is used and disclosed for ethical purposes, protects privacy, cultivates trust and transparency, and fosters the community buy-in necessary for long-term sustainability.

A technological infrastructure to store and exchange data is another common component of CIEs. Data may be stored in a central data repository, or the CIE may act as a message facilitator that enables information sharing across participants.[18] Many CIEs have functionalities to promote interoperability across participants, such as integration with participants' existing data systems.[19] One common component of the technological infrastructure is a longitudinal record, a comprehensive historical record comprising demographic information, health conditions and social needs, past and present services, referral history, and other data.[20] Another is a closed-loop referral functionality that permits bidirectional information exchange between a referring provider and a provider receiving a referral, allowing the referring provider to determine the referral outcome and to follow up as necessary.[21] Finally, CIEs generally permit participants to receive notifications and alerts of a major status change that may result in new care needs, such as an individual who is unhoused being released from jail or discharged from a hospital.[22]

Legal and Policy Challenges

The development and use of a CIE give rise to a host of legal and policy considerations, posing challenges for effective information exchange. A primary legal challenge stems from the diverse array of participants involved in a CIE. Because participants come from different sectors and hold different types of data, they are not all uniformly covered by the same privacy laws. Use and disclosure of data through a CIE will thus be governed by a patchwork of different legal requirements, at times distinct and at times overlapping. Understanding and complying with such requirements can be an arduous endeavor.[23] And, while many privacy laws permit use or disclosure with an individual's consent, they typically establish requirements with respect to what a valid consent must include, creating challenges for the development of a single consent form and process.[24]

The agreement structure formalizing the relationships among parties is also shaped by legal requirements governing agreement type and content, which may vary depending on the type of party at hand (e.g., health care provider, social services agency, third party vendor).[25] Lastly, CIEs implicate a number of critical policy decisions related to privacy and confidentiality safeguards, and require robust data governance and ethical data stewardship practices to cultivate trust and transparency and prevent harmful uses of data. Personal, and at times sensitive, information is shared through a CIE, and misuse can lead to negative repercussions, discouraging people from accessing care, undermining trust in support networks, and harming individuals, all of which impede the goals of a CIE. A CIE's policies, procedures, and practices can help to ensure that data is only used and disclosed in ways that protect and promote the health of community members. These decisions are determined by legal requirements, as well as ethical standards, practical considerations, and the perspectives of key partners — most crucially, directly impacted communities with lived experience navigating systems of health and social care.

Developing CIE Legal Frameworks

Legal Framework Goals for CIEs

Creating a legal framework for a CIE often involves serving several goals. Most notably, the legal framework must facilitate the exchange of data to support articulated use cases within the CIE, such as serving the needs of older adults or individuals experiencing homelessness. A CIE legal framework should also ensure that data is protected throughout the data life cycle. The framework should therefore ensure the data is handled responsibly by authorized individuals, in a manner that safeguards the confidentiality, integrity, and availability of the data.[26] Finally, a clear legal framework should provide needed transparency and accountability, foster trust in the CIE, and promote participation by individuals, the community, and CIE participating organizations alike.

A Strong CIE Legal Framework Requires Clearly Articulated Data Flows to Support Unambiguous Use Cases

Because the data flows are central to strong legal frameworks, time will be well spent analyzing the data flows, such as with a data flow map, and considering the legal questions presented through these data flows. A data flow map may identify not just the flow of data, but the direction of the movement of data, who will interact with the data, and at which points data may be encrypted. These questions might include how data subject to different regulatory requirements may be exchanged between partners who are subject to differing regulatory obligations to facilitate specific use cases. For example, a hospital or FQHC will likely be a covered entity[27] under HIPAA, while a shelter, food and nutrition program or other social services

https://doi.org/10.1017/jme.2026.10238 Published online by Cambridge University Press

provider will, in all likelihood, not be subject to HIPAA because they do not meet the definition of covered entity. Protected health information[28] (PHI) of a covered entity is subject to HIPAA privacy standards, while similar or even the same data in the hands of a non-covered entity may not be subject to HIPAA and may be subject to a different legal and regulatory framework entirely. For example, some social services providers may be subject to federal and state laws protecting confidentiality of victims of abuse. Other agencies might be subject to federal and state protections around the confidentiality of substance use disorder treatment. Finally, a local Supplemental Nutrition Program for Women, Infants, and Children (WIC) agency is subject to the confidentiality provisions within the WIC regulations.[29]

In this context, a use case describes a specific scenario in which data is exchanged through the CIE to achieve a stated purpose and is key to identifying relevant legal questions and considerations. A CIE use case might include, for example, coordinating respite care for people experiencing homelessness.

Developing a data flow map, showing how data will be exchanged — when, by whom, for what purpose, and at what point — and clearly articulating use cases are thus foundational steps in developing a CIE legal framework.

Consent as a Foundation for CIEs

Leading with Consent

As noted above, CIEs permit health care providers, social service agencies, community-based organizations, and government agencies to share individually identifiable information to coordinate care and services to individuals. CIEs typically rely on an individual's express consent to share their information, as the individually identifiable, multi-sector, and real-time data sharing in a CIE is virtually impossible without consent.[30]

This contrasts with many other data sharing initiatives, which do not obtain an individual's consent to share data. Consent may not be legally required if certain exceptions are met and procuring consent can render many data sharing collaborations operationally infeasible if it must be obtained from thousands — or millions — of individuals. When determining whether obtaining consent is necessary, partners must carefully evaluate laws and regulations governing data, and structure data sharing initiatives accordingly.

The consent-based model of CIEs can simplify the legal framework for data sharing when compared to legal frameworks rooted in applicable exceptions to the need for consent. Obtaining consent can also foster trust and provide an opportunity for greater community buy-in.

Developing a Legally Compliant Consent Model

As a first step in developing a consent model, the backbone entity should evaluate the partners participating in a CIE and the types of data they will be sharing. CIEs should determine whether they exchange sensitive information, such as mental health or substance use disorder (SUD) information, as this may trigger specific federal and state legal requirements on consent.[31] For example, HIPAA and 42 CFR Part 2 (Confidentiality of Substance Use Disorder Patient Records, hereafter "Part 2"), as well as state law, have specific elements and statements required in consent.[32] HIPAA also lists circumstances in which an authorization is invalid — such as if the expiration date has passed or the document is incomplete — and prohibits, with some exceptions, combining consents with other documents to create a compound authorization.[33] Part 2 imposes heightened confidentiality on how SUD treatment records maintained by Part 2 programs can be disclosed or used. CIEs must identify when Part 2 applies and craft consent accordingly. Alternatively, some CIEs will share information with Part 2 programs but do not receive any information from Part 2 programs.[34] Under these circumstances, having a Part 2 compliant consent is not needed.

In addition to the legal considerations, there are also equitable issues that a CIE will need to address in its consent model. For example, there is often a power imbalance between a provider and the individual seeking services. Acknowledging and finding effective ways to mitigate this power differential to ensure that consent is voluntary can promote equity in a CIE. Methods include accurately conveying that treatment or services will not be withheld if they refuse to sign the consent, as well as involving individuals and community in the CIE design process. Involving people with lived experience, such as community health workers, in the consent encounter can support culturally competent communication of the risks, benefits, and terms of data sharing and further mitigate the power differential.

Managing consent also raises numerous technological and procedural challenges. CIEs will want to ensure that their technology and procedures are harmonized with their consent model, including how consent is recorded or revoked. Most everyone whose information is shared in a CIE has an initial touchpoint with a provider (whether healthcare, social services, or other type of provider) when seeking treatment or services, making this a natural point of contact to obtain consent.[35] Having uniform procedures to explain consent and answer questions about the CIE can promote consistency in operations.[36]

Best Practices for Consent Generally

There are several identified best practices that generally apply when seeking an individual's consent to share their personal information.[37]

Signing the consent should be voluntary, not a condition of receiving treatment, referrals, or services. Programs should articulate this principle plainly — both in the consent document and in staff scripts — to minimize coercion and ensure that clients understand their options. Staff should also ensure that individuals have capacity to consent, and if needed, provide support to achieve capacity. Capacity includes verifying the individual is legally permitted to consent. Variables such as the age of the person, their mental and physical state, and state and federal laws may affect capacity.

Consent materials should be concise, readable, and drafted in plain language. The consent form should explain what information may be shared with whom, and for what purposes, to ensure informed consent. If needed, consent forms should be translated into languages besides English and made accessible for individuals with disabilities. Where highly sensitive data is involved, separate, affirmative consent may be appropriate or legally required.

Programs should capture consent by an affirmative act such as a signature, e-signature, or checkbox. Individuals should be permitted to revoke consent at any time, although revocation generally only affects future sharing, not information previously disclosed. Furthermore, consent should have a reasonable expiration date. Lastly, programs should also evaluate whether material changes to data uses or recipients require new consent. This type of transparency with respect to operational changes strengthens community trust.

https://doi.org/10.1017/jme.2026.10238 Published online by Cambridge University Press

Key Features in CIE Consent Models

The Network for Public Health Law conducted a landscape survey of consent models across CIEs to distill key features. While there was some variability, similarities prevailed with most of the best practices described above being present.

Every consent model contained language stating that signing the consent form was voluntary and will not impair the individual's ability to access services.[38] A few noted that declining to sign could make it harder to coordinate care for the individual.[39] All CIE consent documents specified the categories of data to be shared, the categories or names of recipient organizations, and the purposes of use and disclosure (for example, care coordination, providing services, and making referrals), thus advancing informed consent.[40]

All consents also had an expiration date embedded in the document along with a statement about the individual's right to revoke the consent at any time.[41] Where sensitive information is implicated — particularly mental health, HIV status, or SUD records — consent models usually required an additional explicit authorization.[42]

Many consents listed clients' rights or had this information in a distinct section, which often contained a statement on the voluntariness of signing — along with rights of access, rights to request a copy of information, complaint processes, right to an accounting of disclosures, or other options that may be offered by the CIE.[43] Some CIEs also offered tiered options for information sharing, such as basic versus sensitive data, or limiting disclosures to only certain providers.[44] Tiered consent allows individuals to exercise greater autonomy and control over their information.

At least one CIE had a multi-party consent, which allowed people to sign one form to share their information with two different data systems.[45] All forms were relatively brief, generally about two to four pages, and strove to balance brevity with adequate information.

Finally, consent is not only a document, but also a workflow. As such, CIEs will want to review their policies and procedures and standardize processes around staff training; documentation; the modality of capturing consent, such as electronic or paper; and revocation. Engaging the community to review the consent model and meaningfully incorporating feedback can promote equity and enhance community trust and support for the CIE. Furthermore, many organizational participants in a CIE will have existing consent processes. Ideally, the CIE can leverage the expertise of its partners to develop an equitable and legally compliant consent model.

Harmonizing CIEs with HIPAA

HIPAA is by no means the only privacy law applicable to CIEs. On the contrary, other laws, both federal and state, may apply that limit or restrict which types of data are exchanged through a CIE, when they are exchanged, and for which purposes. There may be specific or general privacy laws applying to such categories as health information generally,[46] medical records,[47] breaches of system data,[48] mental health information,[49] and substance use data.[50] All such laws should be analyzed when developing a CIE legal framework to determine their impact on proposed data flows. HIPAA is nevertheless one of the most detailed health privacy laws in the US, and while it is a law of limited jurisdiction, it applies to the PHI of all covered entities and their business associates. HIPAA thus carries huge implications for CIEs that include covered entities — such as hospitals, FQHCs or other HIPAA-covered health care providers, health plans (including Medicaid), and health care clearinghouses.[51]

The overarching challenge is how to fit disclosures of data envisioned for a CIE within the permissible uses and disclosures of PHI under HIPAA's Privacy Rule.[52] HIPAA, a law enacted in 1996, and its corresponding Privacy Rule finalized on December 28, 2000, predates the more contemporary concept of a CIE. Because of the relative novelty of CIEs and their focus on *cross-sector* data sharing, applying the HIPAA Privacy Rule to CIEs can feel like trying to fit a square peg in a round hole. However, the HIPAA Privacy Rule is flexible.[53] This flexibility is found "particularly in the implementation specifics for making the minimum necessary uses and disclosures," for example.[54] The US Department of Health and Human Services (HHS) has similarly described the Privacy Rule requirement to apply appropriate safeguards to PHI to be "flexible and scalable."[55]

Many disclosures by covered entities to other participants in a CIE, even non-HIPAA-covered entities, fall squarely within HIPAA's permitted uses and disclosures for treatment, payment, and health care operations.[56] The nuanced role of a CIE backbone entity, however — which may include facilitating data exchange among HIPAA-covered entities and non-HIPAA-covered entities alike, data governance, generating and maintaining a longitudinal record, creating and maintaining a master patient index (MPI), or standardizing data formats — requires careful analysis to reconcile such functions and data flows with the requirements of the HIPAA Privacy Rule. A backbone entity that is neither a health plan, covered health care provider, nor health care clearinghouse is not a covered entity.[57] So, how then do HIPAA-covered health care providers, health plans, and health care clearinghouses play in the CIE sandbox, allowing access to their PHI by a CIE backbone entity that provides neither treatment, payment, nor health care operations functions and is not itself a covered entity? And how does the CIE legal framework resolve this? The answer may lie in HIPAA's treatment of business associates, such as Health Information Organizations (HIOs).

The CIE Backbone Entity as an HIO or Other Business Associate

Since it was first finalized in 2000, the HIPAA Privacy Rule has included a two-part definition of business associate.[58] First, a business associate relationship arises "when the right to use or disclose the [PHI] belongs to the covered entity, and another person is using or disclosing the [PHI] (or creating, obtaining and using the [PHI]) to perform a function or activity on behalf of the covered entity."[59] Second, the Privacy Rule enumerates specific services, such as legal, actuarial, or data aggregation, which create a business associate relationship "where the provision of the services involves the disclosure of [PHI] from such covered entity… or from another business associate of such entity… to [a] person."[60]

In addition to these broad groups, HIPAA also expressly calls out certain types of entities as business associates.[61] Health information organizations were expressly identified as business associates after the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. Section 17938 of that Act states:

> Each organization, with respect to a covered entity, that provides data transmission of [PHI] to such entity (or its business associate) and that requires access on a routine basis to such [PHI], such as a[n] [HIO], [or] Regional [HIO],… is required to enter into a [business associate agreement], with such entity and shall be treated as a business associate of the covered entity for purposes of the provisions of [the HIPAA Security and Privacy Rules].[62]

https://doi.org/10.1017/jme.2026.10238 Published online by Cambridge University Press

Since the rule was first finalized, HHS has made clear that a mere "conduit" for PHI is not a business associate.[63]

> A conduit for PHI transports information but does not access [PHI] other than on a random or infrequent basis as may be necessary for the performance of the transportation service, or as required by law.[64]

In some cases, then, whether an entity that transports PHI is a mere conduit may determine whether it is a business associate.

> Entities that manage the exchange of [PHI] 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 [PHI].[65]

> A[n] [HIO] that manages the exchange of [PHI] through a network on behalf of covered entities... is not considered a conduit and, thus, is not excluded from the definition of business associate.[66]

All CIEs are different and counsel for CIEs, in the process of developing a legal framework, should carefully analyze whether the CIE backbone entity in question meets the definition of business associate — either as an HIO, or because it fits within other parts of the definition of business associate as described above. The legal analysis should determine if the CIE backbone entity "on behalf of" the covered entities "creates, receives, maintains or transmits PHI" or if it provides one or more of the enumerated functions found in the definition of business associate discussed above, such as "legal, actuarial [or] data aggregation."[67]

A key consideration will be whether the CIE backbone entity is a mere conduit for PHI, having no more than random access to PHI. The functions of the CIE will be material to that analysis, in addition to whether, and the degree to which, the CIE backbone entity has access to PHI on behalf of one or more covered entities.

Further, the legal analysis should delve into HIPAA's treatment of HIOs to determine whether the CIE backbone entity is itself an HIO. The term Health Information Organization does not have a set definition within HIPAA, with HHS reasoning it intentionally did not define the term because "the industry continues to develop and thus the type of entities that may be considered [HIO]s continues to evolve."[68] However, HHS has said that HIO "is a more widely recognized and accepted term to describe an organization that oversees and governs the exchange of information among organizations."[69]

Thus, counsel should analyze whether the CIE backbone entity "provides data transmission of [PHI] to such entity (or its business associate) and whether that requires access on a routine basis to such [PHI]."[70] Similarly, the legal analysis should consider, for example, whether the CIE backbone entity "manages the exchange of [PHI] through a network on behalf of covered entities."[71]

Authorities Granted to a CIE Backbone Entity

The HIPAA Privacy Rule and Security Rule require covered entities and business associates to execute agreements with their business associates to safeguard the PHI they handle, and apply many of HIPAA's provisions to the business associates.[72]

> The Privacy Rule would permit a[n] HIO, acting as a business associate of one or more covered entities, to make any disclosure the covered entities are permitted by the Privacy Rule to make, provided the HIO's business associate agreement(s) authorizes the disclosure.[73]

> In most cases, the permitted uses and disclosures established by a business associate agreement will vary based on the particular functions or services the business associate is to provide the covered entity.[74]

> A[n] HIO can operate as a business associate of multiple covered entities participating in a networked environment. [T]he Privacy Rule would not require separate business associate agreements between each of the covered entities and the business associate.[75]

In that scenario, each of the covered entities and the business associate would be parties to the same business associate agreement.[76] Which authorities the business associate agreement specifically delegates to the HIO or other business associate will depend on factors such as the nature of the CIE and data flows, responsibilities of the business associate, and "any other legal obligations on covered entities and/or HIOs with respect to the PHI in the network."[77]

> For example, the business associate agreements between covered entities and a[n] HIO may authorize the HIO to: manage authorized requests for, and disclosures of, PHI among participants in the network; create and maintain a master patient index; provide a record locater or patient matching service; standardize data formats; implement business rules to assist in the automation of data exchange; facilitate the identification and correction of errors in health information records; and aggregate data on behalf of multiple covered entities.[78]

> If the HIO will primarily manage the exchange of PHI among participating entities for treatment purposes, then the parties should, in the business associate agreement, define the HIO's permitted uses and disclosures of PHI with those limited purposes in mind.[79]

In addition to outlining the specific authorities granted to the business associate, for a number of reasons, covered entities and business associates may also wish to limit those authorities. The most obvious of these reasons is that HIPAA strictly limits uses and disclosures of PHI, particularly when an authorization or opportunity to agree or object is not required.[80] Covered entities and business associates also have to comply with HIPAA's minimum necessary rule. That rule requires a covered entity — when using, disclosing, or requesting PHI — to (in many but not all instances) use, disclose, or request only the minimum necessary amount of information to complete the intended purpose.[81] Counsel who determine their CIE backbone entity to be a business associate of one or more covered entities, either as an HIO or other business associate, should carefully consider the different authorities that may be granted to the backbone entity through the business associate agreement (or other arrangements permitted under the Privacy Rule).[82]

Special consideration should be given, for example, to those instances and functions requiring access to unencrypted PHI. Attention should be given to whether the CIE backbone entity maintains PHI on behalf of the covered entities in a longitudinal record, and whether, on behalf of the covered entities, it releases any of this or other PHI to authorized persons and entities. Some CIEs may use a master patient index, record locator service, or application programming interfaces, which may require access to PHI, and this too should be considered in determining authorities granted to the CIE backbone entity.

Each of the functions requiring access to PHI, and other obligations with respect to the PHI placed on the business associate by the covered entity or other business associate, should be reflected in the authorities granted to the CIE backbone under the agreement. The agreement or other arrangement should, as in the case of all business associate agreements, include HIPAA's required elements for a business associate agreement, such as the need to safeguard all PHI against unauthorized uses and disclosures.[83]

https://doi.org/10.1017/jme.2026.10238 Published online by Cambridge University Press

Conclusion

As the health and social services fields increasingly explore opportunities for collaboration to provide whole-person care addressing health and health-related social needs, CIEs present a pathway to unite cross-sector partners through information sharing that is community driven and equity centered. CIEs implicate a host of legal and policy issues, as they necessitate robust data governance to ensure that information sharing complies with legal and ethical standards. While CIEs present some novel challenges for counsel developing legal frameworks, this article has identified considerations, best practices, and lessons learned that can guide counsel in this ambitious endeavor, with close analysis of two crucial framework components — consent models and HIPAA compliance. With a strong legal framework, the backbone entity, participating organizations, and community members have the foundation for trusted and accountable information sharing central to CIEs.

Acknowledgements. The authors would like to thank the Illinois Public Health Institute for their collaboration and partnership on the Chicago Regionwide CIE, which informed the development of this paper.

Disclosure. The Robert Wood Johnson Foundation provided support for the Network for Public Health Law's contributions to this article and participation in a conference presentation on the same topic. The Network for Public Health Law conducted a legal analysis on questions similar to those addressed in this article under a contract with the Illinois Public Health Institute. The views expressed are those of the authors and do not necessarily reflect the views of the Robert Wood Johnson Foundation or the Illinois Public Health Institute.

Stephen Murphy, JD, is a public health attorney and Director of the Network for Public Health Law's Mid-States Region Office.

Meghan Mead, JD, is a Deputy Director at the Network for Public Health Law's Mid-States Region Office, with expertise in public health data and data sharing.

Emma Kaeser, JD, is a public health lawyer and staff attorney at the Network for Public Health Law.

References

1. "Healthy People 2030, Social Determinants of Health Literature Summaries," US Department of Health and Human Services, https://odphp.health.gov/healthypeople/priority-areas/social-determinants-health/literature-summaries (last visited January 12, 2026).
2. "Healthy People 2030, Food Insecurity," US Department of Health and Human Services, https://odphp.health.gov/healthypeople/priority-areas/social-determinants-health/literature-summaries/food-insecurity (last visited January 12, 2026).
3. "Healthy People 2030, Access to Health Services," https://odphp.health.gov/healthypeople/priority-areas/social-determinants-health/literature-summaries/access-health-services (last visited January 12, 2026).
4. National Academies of Sciences, Engineering, and Medicine, *Integrating Social Care into the Delivery of Health Care* (National Academies Press, 2019): at 1–2, https://doi.org/10.17226/25467.
5. Caroline Fichtenberg, et al., "Health and Human Services Integration: Generating Sustained Health and Equity Improvements," *Health Affairs* 39, no. 4 (2020): 567–73, at 569–70, https://doi.org/10.1377/hlthaff.2019.01594.
6. Fichtenberg, "Health and Human Services Integration," at 567–68; National Academies of Sciences, Engineering, and Medicine, *Integrating Social Care*, at 1–2.
7. "What is CIE?," CIE San Diego, https://ciesandiego.org/what-is-cie/ (last visited January 12, 2026).
8. *See, e.g.*, "Social Health Information Exchange," Alameda County Health, January 2025, https://accareconnect.org/wp-content/uploads/2025/04/SHIE-One-Pager-Jan-2025-draft-v2.pdf (last visited January 12, 2026).
9. *See, e.g.*, "CIE Partners," CIE San Diego, https://ciesandiego.org/partners/#ciepartners (last visited January 12, 2026).
10. Camey Christenson, et al., *Collaboration and Cross-Sector Data Sharing to Create Healthier Communities* (211 San Diego and CIE San Diego, November 2018): at 7, https://ciesandiego.org/toolkit/ (last visited January 12, 2026).
11. Alana Kalinowski, et al., *Community Information Exchange: Leveraging Collaborative Infrastructure to Assess and Address ACES* (211 San Diego, CIE San Diego, San Diego Accountable Community for Health, YMCA, Partners in Prevention 2021): at 8, 14, https://ciesandiego.org/2021/10/30/community-information-exchange-leveraging-collaborative-infrastructure-to-assess-and-address-aces/ (last visited January 12, 2026).
12. Machell Town, et al., "Racial and Ethnic Differences in Social Determinants of Health and Health-Related Social Needs Among Adults — Behavioral Risk Factor Surveillance System, United States, 2022," *Morbidity and Mortality Weekly Report* 73, no. 9 (2024): 204–8, http://doi.org/10.15585/mmwr.mm7309a3; Nambi Ndugga, et al., "Key Data on Health and Health Care by Race and Ethnicity," KFF, June 11, 2024, https://www.kff.org/racial-equity-and-health-policy/key-data-on-health-and-health-care-by-race-and-ethnicity/?entry=executive-summary-introduction#experiences-with-racism-discrimination-and-unfair-treatment (last visited January 12, 2026).
13. *See, e.g.*, "About Us," Chicago Regionwide CIE, https://www.chicagoregionwidecie.org/about-us (last visited January 13, 2026).
14. *See, e.g.*, "Community Voice," CIE San Diego, https://ciesandiego.org/community-voice/ (last visited January 13, 2026).
15. *See, e.g.*, "Participation Agreement," HealthierHere, https://www.healthierhere.org/library/participation-agreement (last visited January 13, 2026).
16. "CIE Clients," North Coast Health Improvement and Information Network, https://www.nchiin.org/cie-clients/ (last visited January 13, 2026).
17. *See, e.g.*, HealthierHere, "Connect2 Community Network Plan," https://www.healthierhere.org/library/making-way-for-a-connected-system-the-connect2-community-network-plan, (last visited January 13, 2026).
18. Christenson, et al., *Collaboration and Cross-Sector Data Sharing*: at 6; Lily Doher, Sue McGuire, and Bob Kreha, "Community Information Exchange Privacy and Technology," United Way for Southeastern Michigan, YouTube, August 24, 2023, 15 minutes, https://www.youtube.com/watch?v=xjSzr8ucZfM (last visited January 13, 2026).
19. *See, e.g.*, Christenson, et al., *Collaboration and Cross-Sector Data Sharing*: at 4.
20. *See, e.g.*, Christenson, et al., *Collaboration and Cross-Sector Data Sharing*: at 6.
21. *See, e.g.*, "CommunityCares," Arizona Health Care Cost Containment System, https://www.azahcccs.gov/communitycares (last visited January 13, 2026).
22. *See, e.g.*, "NCCC User Tip of the Week: Managing Alerts and Notifications," North Coast Health Improvement and Information Network, https://www.nchiin.org/2025/07/10/nccc-user-tip-of-the-week-managing-alerts/ (last visited January 13, 2026).
23. Alexander Dworkowitz and Cindy Mann, *Data Sharing and the Law: Overcoming Healthcare Sector Barriers to Sharing Data on Social Determinants*, (Manatt Health and Social Interventions Research & Evaluation Network, July 2020): at 4, https://sirenetwork.ucsf.edu/tools-resources/resources/data-sharing-and-law-overcoming-health-care-sector-barriers-sharing-data (last visited January 13, 2026).
24. *Compare* 45 C.F.R. § 164.508 (2024) *and* 42 C.F.R. Part 2 Subpart C (2024).
25. *See, e.g.*, 45 C.F.R. § 164.504(e) (2024).
26. *See, e.g.*, "Your Privacy is Important to US," CIE San Diego, https://ciesandiego.org/privacy/ (last visited January 13, 2026); "Enabling Patients and the Health Care Community," Contexture, https://contexture.org/patient-rights/ (last visited January 13, 2026).
27. 45 C.F.R. § 160.103 (2024).
28. 45 C.F.R. § 160.103 (2024).
29. 7 C.F.R. § 246.26(d) (2025).
30. Christenson, et al., *Collaboration and Cross-Sector Data Sharing*: at 35; 211 San Diego, *What is a Community Information Exchange (CIE)?*, (Assistant Secretary for Technology Policy, 2024), ONC_SDOH_Learning_Forum_Workshop_3_211_CIESanDiego_FINAL_06262024.pdf, (last visited January 13, 2026).

https://doi.org/10.1017/jme.2026.10238 Published online by Cambridge University Press

31. *See generally* 45 C.F.R. Part 160 and 164 (2024); 42 C.F.R. Part 2 (2024).
32. 45 C.F.R. § 164.508 (2024).
33. 45 C.F.R. 164.508(b) (2024).
34. *See, e.g.*, Resource Connection Network, *Consent to Share Personal Information* (Sonoma Connect | Sonoma Unidos), https://drive.google.com/file/d/1pm20lawyvAMQvwhMz54NaK1JOsBPpfdi/view (last visited January 13, 2026).
35. *See generally* Christenson, et al., *Collaboration and Cross-Sector Data Sharing.*
36. Community Information Exchange, *Community Information Exchange Best Practices for Discussing the CIE Authorization form and FAQs* (211 San Diego), https://ciesandiego.org/wp-content/uploads/2019/08/Best-Practices-FAQ.pdf (last visited January 13, 2026).
37. *See generally* Daniel Stein et al., *Catalyzing Whole-Person Care: Consent-to-Share is the Key Insights, Next Steps and a Roadmap* (Stewards of Change Institute, 2024), https://stewardsofchange.org/ (last visited January 13, 2026).
38. Connect2 Community Network, *Privacy Framework* (HealthierHere, April 2, 2023), https://www.healthierhere.org/library/connect2-privacy-framework (last visited January 13, 2026).
39. Resource Connection Network, *Consent to Share Personal Information.*
40. Connect2 Community Network, *Privacy Framework.*
41. North Coast Care Connect, *Authorization For The Use And Disclosure* (North Coast Health Improvement and Information Network, 2024), https://www.nchiin.org/cie-clients/ "NCCC Consent Form", (last visited January 13, 2026).
42. Alameda County Health Care Services Agency, *Alameda County Information Sharing Authorization* (Alameda County Care Connect), https://accareconnect.org/wp-content/uploads/2021/10/20200925_ISA_v3_final.pdf (last visited January 13, 2026).
43. North Coast Care Connect, *Authorization For The Use And Disclosure.*
44. Resource Connection Network, *Consent to Share Personal Information.*
45. San Diego County Homeless Management Information System, *Multiparty Authorization to Use and/or Disclose Information* (Regional Task Force on Homelessness), https://www.rtfhsd.org/wp-content/uploads/2024/09/HMIS-CIE-Multiparty-Authorization-Final-7.06.2022.pdf (last visited January 13, 2026).
46. *See, e.g.*, Illinois Medical Patient's Rights Act, 410 Ill. Comp. Stat. 50/3.1.
47. *See, e.g.*, California Medical Information Act, Cal. Civ. Code § 56.10 (West).
48. *See, e.g.*, Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. 530/.
49. *See, e.g.*, Illinois Mental Health and Developmental Disabilities Confidentiality Act, 740 Ill. Comp. Stat. 110/.
50. *See, e.g.*, 42 C.F.R. Part II (2024).
51. *See* 45 C.F.R. § 160.103 (2024) (defining covered health care provider, health plan and health care clearinghouse).
52. 45 C.F.R. Subpart E (2024).
53. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82462, 82782 (Dec. 28, 2000) ("[W]e believe that the flexible approach under this rule is more efficient and appropriate then a single approach to safeguarding health information privacy.")
54. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82462, 82471 (Dec. 28, 2000).
55. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82462, 82746 (Dec. 28, 2000).
56. *See* 45 C.F.R. § 164.506 (2024).
57. *See* 45 C.F.R. § 160.103 (2024) (defining covered entity).
58. 45 C.F.R. § 160.103 (2024). *See also* Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82462, 82746 (Dec. 28, 2000).
59. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82462, 82475 (Dec. 28, 2000). *See also* 45 C.F.R. § 160.103 (2024).
60. 45 C.F.R. § 160.103 (2024).
61. 45 C.F.R. § 160.103 (2024).
62. 42 U.S.C. § 17938 (2023).
63. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 82462, 82746 (Dec. 28, 2000).
64. Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information.*
65. 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).
66. 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*, at 5572.
67. *See* 45 C.F.R. § 160.103 (2024).
68. 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).
69. 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).
70. *See* 42 U.S.C. § 17938 (2010).
71. 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).
72. 45 C.F.R. § 164.308(b) (2024); 45 C.F.R. § 164.502(e) (2024).
73. Office for Civil Rights, "To what extent does the HIPAA Privacy Rule allow third parties to access protected health information (PHI) through a health information organization (HIO) for purposes other than treatment, payment, and health care operations?," US Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/547/to-what-extend-does-hipaa-allow-third-parties-to-access-information/index.html (last visited January 13, 2026).
74. Office for Civil Rights, "What may a HIPAA covered entity's business associate agreement authorize a health information organization (HIO) to do with electronic protected health information (PHI) it maintains or has access to in the network?," US Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/543/what-may-a-covered-entitys-business-associate-agreement-authorize/index.html (last visited January 13, 2026).
75. Office for Civil Rights, "Can a health information organization (HIO) operate as a business associate of multiple covered entities participating in a networked environment?," US Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/560/can-an-hio-operate-as-a-business-associate-of-multiple-covered-entities/index.html (last visited January 13, 2026).
76. Office for Civil Rights, "Can a health information organization (HIO) operate as a business associate."
77. Office for Civil Rights, "What are some considerations in developing and implementing a business associate agreement with a health information organization (HIO)?," US Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/561/what-are-some-considerations-in-developing-and-implementing-a-business-associate-agreement/index.html (last visited January 13, 2026).
78. Office for Civil Rights, "What may a HIPAA covered entity's business associate agreement authorize a health information organization (HIO) to do with electronic protected health information (PHI) it maintains or has access to in the network?," US Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/543/what-may-a-covered-entitys-business-associate-agreement-authorize/index.html (last visited January 13, 2026).

https://doi.org/10.1017/jme.2026.10238 Published online by Cambridge University Press

79. Office for Civil Rights, "What are some considerations in developing and implementing a business associate agreement with a health information organization (HIO)?," US Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/561/what-are-some-considerations-in-developing-and-implementing-a-business-associate-agreement/index.html (last visited January 13, 2026).
80. 45 C.F.R. § 164.512 (2024).
81. 45 C.F.R. § 164.502(b) (2024).
82. 45 C.F.R. § 164.504(e) (2013).
83. *See* 45 C.F.R. § 164.504(e)(2)(ii) (2024).

https://doi.org/10.1017/jme.2026.10238 Published online by Cambridge University Press