Considerations for Privacy and Security of Statewide CIE

Purpose

The Community Information Exchange (CIE) Workgroup has been tasked by the Health Information Technology Oversight Council (HITOC) under House Bill 4150 (2022) with exploring strategies to accelerate, support, and improve statewide CIE in Oregon.

The CIE Workgroup met in September 2022 to discuss privacy and security of statewide CIE. The discussion generated guiding principles and initial privacy and security considerations for CIE in Oregon. This concept paper is a result of those discussions and will be reviewed by HITOC in December to inform their HB 4150 final report to the legislature in January 2023.

Context

When widely adopted across the state, CIE can help eliminate many of the barriers between people and the services designed to support them. It enables a broad variety of service providers to connect easily and quickly to organizations across the health and social service spectrum. Organizations can search a shared resource directory for appropriate services, send timely referrals, and receive feedback on whether the services were provided, a process known as "closing the loop". CIE can save consent, demographic, and other types of information to help coordinate services. The information from CIE can also be leveraged to improve the health and social care systems and support equity in service delivery. Ensuring privacy and security of this information is a critical consideration for CIE efforts in Oregon, as well as important for building trust with individuals and communities.

Privacy generally refers to an individual's ability to keep certain personal information free from unauthorized access and the ability to access and share the information themselves.

Security is the way organizations control access and protect this information, including safeguarding it from accidental or intentional disclosure.*

Since CIE encompasses a wide variety of social service, health, and additional partners who need to collect and exchange different types of information to coordinate care, multiple laws (e.g., HIPAA, FERPA, 42 CFR Part 2, and FTC regulations[1]) and standards may apply to how information is handled in CIE. This information may include identifying, demographic, physical health, behavioral health, or other sensitive information, in addition to the social needs and services information necessary for CIE. CIE partners may encounter types of information new to them and requirements they are unfamiliar with. Moreover, individuals may have expectations about how their information is handled that differ from the legal requirements for its use. These standards, expectations, and legal requirements for different types of

[1] HIPAA-Health Insurance Portability and Accountability Act; FERPA-Family Educational Rights and Privacy Act; 42 CFR Part 2-Confidentiality of Substance use Disorder Patient Records; FTC-Federal Trade Commission

*https://www.healthit.gov/playbook/privacy-and-security/

information and organizations create a complex environment for CIE partners and individuals being served. This complexity will need to be considered as CIE efforts continue and laws and standards evolve.

Summary of privacy and security principles and considerations

The CIE Workgroup recommends several privacy and security guiding principles as well as considerations for statewide CIE.

The following outlines **privacy and security principles** to guide statewide CIE in Oregon:

1. **Communities and individuals must guide decisions around collection, storage, sharing, and use of their information:** The CIE Workgroup elevates the need to empower individuals and communities whose information will be shared in CIE to play a central role in guiding decisions about how that information is handled.
2. **CIE systems must adhere to applicable privacy and security laws and should follow national standards:** The CIE Workgroup recommends that statewide CIE efforts adhere to existing and future privacy and security laws as well as to established standards at the national level rather than focus on developing new stand-alone approaches.
3. **Information that will improve services, care, and equity should be collected and shared in CIE:** The Workgroup prioritizes information that will improve service provision, care, and equity, both for the individual being served and the overall health and social care systems. It will be important to be thoughtful about what information to collect to maximize privacy, have sufficient information to provide services easily, and avoid asking individuals repeatedly for the same information.
4. **Transparency on how information will be stored, shared, and used is essential to building trust:** The Workgroup asserts that transparency about what will happen with information individuals provide is critical to ensuring trust. Clear and understandable information on how information will be protected and shared is necessary to achieve this.
5. **Inclusive neutral governance is needed and would include governance of information privacy and security:** The CIE Workgroup recommends including oversight of information privacy and security in the CIE governance process. Members elevate the need for additional working groups with this focus.

The CIE Workgroup also discussed several key areas and puts forth the following initial **considerations**:

- **Types of information in CIE:** In addition to the social needs and services information that must be included for the primary purpose of CIE, the CIE Workgroup feels there is value in collecting and exchanging identifying, demographic, physical health, behavioral health, and sensitive information in CIE, with appropriate safeguards in place.

- **Informed consent:** Informed consent is essential to building trust and maintaining transparency. Members provide considerations on the clarity, frequency, and content of the consent process as important factors to consider in planning for informed consent.
- **Individual access:** Most CIE Workgroup members agreed that individual access should be part of CIE, meaning that individuals could access their own information in CIE, or search for resources and self-refer.

Guiding principles for privacy and security

The CIE Workgroup recommends the following principles to guide decisions about privacy and security in CIE efforts. For example, the principles would be applied to decisions about implementation of CIE technology; privacy and security related governance; types of information; processes for collecting, sharing, and analyzing the information; interactions with individuals being served; and/or agreements between CIE partner organizations. These principles center individuals and communities, their needs and decision-making power, and the safeguarding of personal information that can be shared through CIE.

1) **Communities and individuals must guide decisions around collection, storage, sharing, and use of their information**

   People and communities that will have their information in CIE must guide decisions about how that information is handled. It is important to share the appropriate amount of information so as not to burden a person with re-telling their story or completing repetitive forms, while at the same time protecting and securely exchanging that information, to ensure individuals have access to the services they need. Individuals should also be able to guide decisions around what information is essential to their care and have information corrected when it is wrong. The Workgroup recommends further exploration of allowing individuals to restrict what information they want shared via CIE without disrupting service provision.

   It will be important for communities and individuals to guide how information is used to identify disparities and opportunities for interventions to address them. Workgroup members emphasize that protecting individual privacy is not in conflict with allowing for aggregation of information in CIE to better understand service gaps and opportunities for policy change.

2) **CIE systems must adhere to applicable privacy and security laws and should follow national standards**

   Adherence to established laws, such as HIPAA, FERPA, 42 CFR Part 2, and FTC regulations[2] and aligning CIE systems with national and industry standards are Workgroup

[2] HIPAA-Health Insurance Portability and Accountability Act; FERPA-Family Educational Rights and Privacy Act; 42 CFR Part 2-Confidentiality of Substance use Disorder Patient Records; FTC-Federal Trade Commission

priorities. Monitoring and adapting as laws and standards change will be necessary. Members emphasize relying on these standards rather than redesigning existing regulations and practices, as developing state-specific requirements could be difficult to implement for example. Workgroup members also highlight that many organizations, particularly smaller ones, need support to understand and follow privacy and security laws and standards.

3) **Information that will improve services, care, and equity should be collected and shared in CIE**

When considering what information to include in CIE, decision makers should prioritize information that will improve service provision, care, and equity, both for the individual being served and the overall health and social care system. It will be important to be thoughtful about what information to collect in order to maximize privacy, but still have sufficient information to provide services easily. The Workgroup suggests basing data collection and sharing decisions on necessity and basing data storage decisions on whether there is an ongoing need for the information.

Members also highlight a need to balance privacy protections with client experience to avoid asking individuals repeatedly for the same information. Further consideration should be given to connecting CIE with other data sources to support the collection of minimal information and critical equity goals, while also maintaining privacy.

4) **Transparency on how information will be stored, shared, and used is essential to building trust**

For individuals and communities to trust CIE, it is critical to be transparent about what will happen with the information they provide. One opportunity to achieve this is through a clear, understandable informed consent process. During this, individuals will need clarity about how their information will be stored and shared and what their options are, including the option to opt out of participating in CIE and still receive referrals or services. Staff at organizations using CIE need training on how to have trauma-informed conversations about information sharing, as well as training on privacy and confidentiality laws. Another opportunity to provide transparency is through education with communities, organizations, and individuals around CIE efforts and how it works when implemented. Relationships between organizations and with individuals being served will still be important to building trust.

Informed consent in this context means individuals provide permission for their information to be included or shared within CIE, with an understanding of what will happen with their information in CIE and possible risks and benefits.

See p. 7 for considerations to achieve informed consent.

5) **Inclusive neutral governance is needed and should include governance of information privacy and security**

The CIE Workgroup recommends that inclusive neutral governance include oversight of information privacy and security, likely through a specific group or subcommittee that includes privacy and security experts. Members emphasize this would likely entail an organized process and in-depth procedures to ensure the different types of data collection and methods of information sharing can be accomplished while protecting privacy and security. Members also highlight the need to allow enough time for governance processes to accommodate the complexity of privacy and security issues for CIE in Oregon, and the importance of centering community, CBOs, and individuals impacted in governance decision-making.

Considerations for privacy and security

CIE should support seamless exchange of information between organizations that provide health and social service supports while maintaining privacy and security. The CIE Workgroup highlights the need to balance privacy with timely access to critical information to ensure that people receive the help they need where and when they need it. This is crucial during times of public crisis such as wildfires and pandemics as well as during circumstances requiring urgency for individuals.

The CIE Workgroup puts forth initial considerations and recommends additional exploration of the privacy and security topics below:

Types of CIE information discussed for the context of this paper included examples such as:

- **Identifying**: Name, address, contact information, etc.
- **Demographic**: Age, income, household size, REALD, SOGI*, etc.
- **Health**: Dietary restrictions due to health conditions, etc.
- **Behavioral health**: For delivering community services or referring to behavioral health organizations, etc.
- **Sensitive**: HIV/STI** services, legal services, situations of intimate partner violence, etc.

1) **Types of information in CIE**

The CIE Workgroup discussed types of information that may be collected and exchanged in CIE and considered potential benefits and risks. Social needs information and social services must be included as they are the main purpose of CIE. Additional information may be necessary or helpful for providing services. Types of information considered included identifying, demographic, health, behavioral health, and sensitive information.

- Identifying: The majority of Workgroup members feel identifying information needs to be part of CIE and is necessary to provide services. There may be situations where people need the ability

* Race, ethnicity, language, and disability (REALD); Sexual orientation and gender identity

** Human immunodeficiency virus/sexually transmitted infection to indicate specifically how to contact them, such as an intimate partner violence situation, and this should be considered.

- Demographic: CIE Workgroup members also see significant value in collecting demographic information, and most members feel this information should be part of CIE. Some potential benefits include identifying linguistic or culturally specific services to refer to and leveraging data to ensure equitable access to services. However, the options in technology systems do not always capture people in the way they would like to be represented. Also, people may be concerned that sharing that information would make them less likely to receive services or change how they are treated. Some individuals may only want certain people to see demographic information, such as sexual orientation or gender identity. These potential risks or safeguards should be considered as CIE efforts develop.
- Health and behavioral health: Most Workgroup members also felt that physical health and behavioral health information should be collected and exchanged as part of CIE. Although the Workgroup did not explore this topic in detail, they identified situations where a CIE referral could be more valuable with specific health or behavioral health information. One potential benefit of including these types of information is the improvement in physical and behavioral health outcomes as a result of receiving social services. However, there are implications due to privacy requirements when including this information in CIE. These areas will need to be thoughtfully considered during further exploration.
- Sensitive information: The Workgroup recognizes there may be circumstances where availability of certain information to coordinate services could overly compromise privacy, such as in situations of intimate partner violence or HIV/STI services. In circumstances such as these or similar, privacy takes precedence and CIE should have safeguards in place to handle such information appropriately and protect the individual. However, this should also be balanced against ease of information collection and exchange to minimize barriers for people being served. Regulatory requirements for protections of certain information should also be accounted for as CIE efforts are developed and implemented.

Overall, people accessing social services are asked for their information repeatedly, and in multiple settings. CIE is an opportunity to reduce the frequency that people are asked for the same information, potentially reducing trauma for the individual and stigma around receiving services. Additionally, Workgroup members emphasized that to make CIE valuable, there needs to be enough information provided with a referral to appropriately serve the person and not slow down the provision of services. In general, the more information a social service provider has about a person, the better they can deliver for the individual overall. Workgroup members suggest that further exploration is needed on how to handle various types of information in CIE.

2) **Informed consent**

Informed consent is a critical aspect of CIE efforts and is essential to building trust and maintaining transparency in what will happen with information. The CIE Workgroup highlights clarity, frequency, and content as important factors to consider in planning for the process of informed consent by people served with CIE.

- Clarity: Members emphasized the importance of ensuring that people understand what they are consenting to. Consent information needs to be accessible, readily understandable, and clear. To support these needs, service providers and clinicians should be trained on how to provide consent information clearly. Consent information should be available in a wide variety of languages, in plain language, and through multiple formats including remote/telephone options. The consent process should also include clear information on how to revoke consent to CIE and that individuals can opt out of CIE, but still receive referrals to services. These steps can ensure that people being served are able to make well-informed decisions about whether to consent to CIE.
- Frequency: Members also considered whether consent to participate in CIE should be obtained a single time, before every referral, or somewhere in between. Most members felt that consent should be obtained once, or potentially more than once in certain situations, but not each time there is a referral. They mentioned the importance of balance between the need to obtain consent and the need for expedient referrals. Requiring repeated consent may conflict with the goal of using CIE to reduce barriers to care, as repeated consent could be a burden, especially for someone in crisis who needs help quickly. Rather, a conversation with the individual regarding each referral, even if a consent form is not required each time, may support a person-centered approach. Members suggested that reducing barriers to providing and revoking consent will be important and should allow for both in-person and remote options. The Workgroup indicated that further exploration is needed in this area.
- Content: Determining what details should be included in the informed consent process will also require further discussion and decision-making, but Workgroup members suggest that any informed consent process lay out the options, potential outcomes, and benefits and risks of consenting. It should be clear in the consent process who will have access to the information shared and how protections function to ensure only the appropriate CIE users see certain information. The Workgroup highlighted that additional discussion is needed to explore safeguards to address safety concerns, for instance in the context of intimate partner violence, and how such safeguards should be clearly communicated during the consent process. Members also felt that a universal template or form may be helpful.

3) **Individual access**

   Most CIE Workgroup members agreed that individual access should be part of CIE, meaning that individuals could access their own information in CIE or search for resources and self-refer. This can support transparency as people could see or potentially update their information. Additionally, people could learn about services they may not have known existed, get information, potentially fill out a form in advance, etc. Additional consideration is needed by others on this area.

The Workgroup asserts that CIE systems and processes should ensure that technical components and workflows are built to provide the appropriate information to support both privacy and service delivery. Moreover, organizations need to prioritize privacy and security and staff must be trained to have comprehensive conversations with individuals seeking services about privacy and informed consent in CIE. Access to relevant information to provide quality coordinated services while ensuring privacy are priorities to the Workgroup. As CIE efforts continue, decisions should account for these needs.

Next Steps

The CIE Workgroup provides these guiding principles and initial considerations around privacy and security and recommends that an additional group or groups, including subject matter experts and communities and individuals impacted, continue to explore these questions. In other regions, groups have met regularly for a year or more to explore the nuances around the implementation of CIE. CIE efforts will need to adapt with the landscape and new learnings, and plan as funding and/or technology opportunities arise. The CIE Workgroup recommends allowing time for this process.

The impact of social determinants of health and the importance of connecting to services across health and social services is well established. However, laws and standards related to social service referrals through CIE are still developing, including for privacy and security, leaving many questions to be considered in the future.

You can get this document in other languages, large print, braille, or a format you prefer. Contact Hope Peskin-Shepherd at Hope.Peskin-Shepherd@dhsoha.state.or.us.