Attachment A

Technical and Operational Plan

Fresno County Community Information Exchange

Countywide development of integrated technical, legal, and governance infrastructure to support two pilots focused on Youth Suicide Prevention and the Integration of Home Visitation Services

November 2024

Table of contents

Contents

Executive Summary

The Fresno County Community Information Exchange (CIE) is an innovative initiative aimed at revolutionizing data utilization to improve the well-being of Fresno County residents. Within the CIE initiative, there are two upcoming pilots scheduled for phased development from 2024-26 that are designed to have immediate and tangible results in the community while concurrently developing the founding partnerships, governance, and technical infrastructure which will carry the work into future years of broadening impact.

This technical and operational plan is a living document currently in draft form, intended to serve as a guiding tool for the ongoing development of the Fresno County CIE. It will be iteratively refined and redesigned through active collaboration with CIE partners and the greater Fresno community, ensuring that it remains responsive to evolving needs and perspectives as the initiative progresses.

Fresno CIE Vision, Mission, and Objectives

Vision

To create a data-driven, interconnected community in Fresno County where timely and effective support is provided to those in need.

Mission

Expedite data sharing across sectors to allow for improved communication and coordinated services for students and families in Fresno County.

Objectives

- Develop initial CIE partnerships, governance, legal framework, and technical infrastructure to set the stage for ongoing development.
- Enhance care coordination and expand accessibility to services for Fresno County residents.
- Streamline service delivery and improve outcomes in key areas.
- Foster trust among stakeholders through clear and effective data governance.

Pilot Initiatives

Suicide Prevention

Fresno County acknowledges the severity of the suicide crisis, with approximately 50,000 suicides and an estimated 1.6 million attempts occurring nationwide each year. The CIE is proactively addressing this issue by integrating data from key agencies to provide timely support and resources to individuals at risk. This initiative marks a crucial step towards comprehensive multi-agency mental health care and suicide prevention efforts.

Key Results

- School districts and behavioral health personnel receive real-time notices regarding individuals at risk of suicide and have operational response plans in place.
- Develop technical early-alert infrastructure in Fresno County that will set the stage for additional alert systems to operate at scale across Fresno County.

Home Visitation

The CIE will address inefficiencies in data transparency that have previously hindered home visitation services. This cross-sector data access pilot aims to streamline services, leading to improved outcomes such as increased kindergarten readiness, better maternal mental health, decreased trauma, and more effective service delivery.

Key Results

- Unified case management across Home Visitation programs in Fresno County, enhancing coordination among program teams and providers.
- Insights into service coverage for children and families.
- Reduced overhead in mandatory reporting for case managers, facilitating an increased capacity to serve the Fresno community in the field.
- Real-time, effective reporting for all CIE users.

These efforts are expected to streamline care coordination and accessibility for residents, irrespective of provider, insurance, network, or region. This early work will set the stage for large-scale data sharing and utilization across Fresno County, creating a more interconnected and data-driven community.

Target Populations

Home Visitation Pilot: Children and Families

This initiative focuses on the following target populations:

- **Infants and Toddlers:** Ensuring that the youngest members of the community receive essential health and developmental support from birth through early childhood.
- **Expectant Mothers:** Providing prenatal care and support to expectant mothers to promote healthy pregnancies and early childhood development.
- **Families with Young Children:** Supporting families with children up to age five, offering resources and guidance on parenting, health, and education to foster a nurturing and safe home environment.

Suicide Prevention Pilot: School-Age Youth

This initiative focuses on the following target populations:

- **Elementary School Students:** Identifying at-risk children at an early age to provide timely support and prevent the escalation of mental health issues.
- **Middle School Students:** Addressing the unique challenges faced by pre-teens and early adolescents.
- **High School Students:** Providing resources and support for teenagers dealing with complex emotional and psychological challenges, including depression and anxiety.

Infrastructure

The core Fresno CIE technology will offer a versatile platform designed to promote interoperability and seamless data exchange among diverse partner data systems. Its centralized and scalable system architecture will enable the integration and transformation of records-level data while ensuring role-based access and field-level governance controls, maintaining privacy and security measures for partners and their data. By providing a standardized yet adaptable framework, the Fresno CIE infrastructure can accommodate new partners and data systems as the partnership grows, thereby scaling its capabilities to meet increasing demands.

Future Development: Supporting the Broader Population of Fresno County

Initial pilot initiatives focusing on children, families, and school-age youth are critical first steps in developing a comprehensive CIE that will ultimately support the entire population of Fresno County. By successfully implementing these pilots, the CIE will:

- **Build a Scalable Framework:** Establish a scalable data-sharing infrastructure that can be expanded to include a wider range of services and populations over time.
- **Demonstrate Impact:** Show tangible benefits and improvements in community health and well-being, building the case for broader adoption and investment in the CIE.
- **Foster Collaboration:** Strengthen partnerships and trust among local service providers, community organizations, and government agencies, creating a collaborative ecosystem that benefits all residents.

As the CIE evolves, it will incorporate additional initiatives and services to address the diverse needs of Fresno County's population. This phased approach ensures that the CIE grows sustainably, continuously improving and expanding its impact in the community.

Introduction

Purpose of the Technical and Operational Plan

This Technical and Operational Plan (TOP) is a comprehensive blueprint designed to guide the initial phases of development and implementation for the Fresno County Community Information Exchange (CIE). The primary purpose of the TOP is to establish a detailed framework that supports the technical, partnership, governance, and legal aspects of the CIE, ensuring its success and sustainability. This section outlines the key objectives and goals of the TOP, emphasizing its role in providing a structured, phased approach to building the CIE technology and partnership.

Aligning People, Organizations, and Technology

Building trust among partners is crucial for successful data-sharing efforts. The Fresno CIE will take small, iterative steps in developing data-sharing practices and supportive technology. The initiative will begin with two pilots carefully selected to test crucial elements of the partnership and technical development for future scaling. The approach involves small groups of committed partners engaging in data discovery and limited data sharing before expanding effective practices and incorporating additional partners. The Technical and Operational plan is designed to establish the basis from which this collaboration can grow and, as a results, is anticipated to be a living document meant to develop clear consensus among participating partners related to the technical and operational boundaries of the work they will be engaging in together.

Leadership and Stakeholder Engagement

Leadership driving the Community Information Exchange (CIE) in Fresno County is characterized by committed public health and education officials working in close collaboration to modernize and integrate health and education data systems despite financial and technological challenges. A joint partnership between Fresno County, the Fresno County Office of Education, and Cradle-to-Career Fresno County is actively working to evolve past outdated methods still prevalent in data sharing, such as fax machines and phone calls, and emphasizes the critical need for interoperability to seamlessly exchange data among diverse systems. Though funding remains a significant barrier, the collaborative core team has secured an earmarked $5 million for data system improvements as initial funding. Achieving full interoperability will require a persistent commitment of additional resources and leadership engagement over years of ongoing technical and partnerships development.

Partnership Development

An effective Community Information Exchange rests in its partnership development. The CIE partnership framework is designed to ensure inclusive, transparent, and efficient collaboration among key stakeholders. This section outlines the roles and responsibilities of the Operational Core Team and Pilot Workgroups involved in developing and implementing the CIE.

Fresno CIE Core Team

The Fresno CIE Core Team provides strategic guidance and operational support to the CIE initiative. This team is composed of leadership from key organizations, including Fresno County, Fresno County Office of Education, and Cradle-to-Career Fresno County. The Core Team's primary responsibilities include:

- **Strategic Guidance:** Setting the overall direction and vision for the CIE, ensuring that the initiative aligns with community needs and priorities.

- **Operational Support:** Overseeing day-to-day operations, coordinating activities among partners, and managing resources to support the development and implementation of the CIE.

- **Stakeholder Engagement:** Facilitating communication and collaboration among all stakeholders, fostering a sense of ownership and commitment to the CIE's success.

Fresno CIE Workgroups

To ensure effective integration of data systems and the successful implementation of the CIE, two Fresno CIE Workgroups have been established, focused on the two initial pilot areas. These workgroups are comprised of representatives from organizations whose data systems will be integrated into the CIE during early phases of technical development. The primary objectives of the workgroups are to establish a Minimum Viable Partnership which will provide the foundational governance structures and build the initial technical infrastructure of the CIE. This includes:

- Identifying key technical systems, use cases, and data fields for inclusion in early phases of the CIE technical implementation.
- Defining and executing service level and data-sharing agreements and protocols.
- Supporting pilot tests to ensure successful and effective technical integration and data interoperability.

By leveraging the expertise and resources of the Core Team and Workgroups, the Fresno CIE will build a strong, collaborative foundation that supports sustainable growth and scalability.

Governance and Management

High-level governance of the Fresno County Community Information Exchange (CIE) will be developed in tandem with the Technical and Operational Plan as a distinct but aligned process. Governance of the CIE is a foundational aspect critical to its success and sustainability. Effective governance ensures that the CIE operates with transparency for its partners, and remains inclusive and accountable to the community it serves. This section outlines the steps which are considered best practice in establishing a governance framework that will guide the operations and evolution of the CIE, addressing the following key areas:

1. **Identify and Define Core Governance Principles** Establishing core governance principles is essential for setting the tone and direction of the Fresno CIE. These principles will prioritize community needs, ensuring that the CIE operates transparently, inclusively, and with a strong sense of accountability. By clearly defining these principles, the CIE can build a foundation that aligns with its mission and values, fostering trust and collaboration among all stakeholders.
2. **Establish a Customized Governance Framework** The governance framework for the CIE must be tailored to address the unique needs and priorities of the Fresno community. This involves developing a structure that accommodates local dynamics and stakeholder expectations. A customized governance framework will ensure that the CIE is responsive and adaptable, providing a solid structure for decision-making and operational management.
3. **Representative Joint Governance Team** A key component of the governance framework is the establishment of a Joint Governance Team. This team will be composed of representatives from various organizations that share data and utilize the CIE. By involving diverse stakeholders in the governance process, the CIE can ensure that multiple perspectives are considered, promoting fairness and inclusivity in its operations.
4. **Conflict Resolution Mechanisms** Effective governance requires clear mechanisms for resolving conflicts that may arise between CIE partners. Establishing well-defined conflict resolution processes will help maintain harmony and collaboration within the CIE. These mechanisms should be transparent and

equitable, ensuring that all parties have a fair opportunity to present their concerns and reach mutually agreeable solutions.

5. **Data Stewardship and Privacy** The governance model of the CIE must prioritize data stewardship and privacy, particularly concerning Personally Identifiable Information (PII) and Protected Health Information (PHI). Implementing stringent data protection measures will safeguard the privacy of individuals and maintain the integrity of the CIE. This commitment to data stewardship will build trust among participants and encourage broader participation in the CIE.
6. **Legal and Regulatory Compliance** Ensuring compliance with legal and regulatory requirements is crucial for the CIE's credibility and functionality. The governance framework must include mechanisms to monitor adherence to data sharing frameworks, policies, procedures, and guidelines. Additionally, it should outline processes for addressing breaches or noncompliance to protect the interests of all CIE participants and maintain the system's integrity.
7. **Regular Governance Review and Adaptation** Governance practices must evolve to remain effective and relevant. Implementing a process for regular review and adaptation of governance practices will ensure that the CIE continues to meet the changing needs of its participants and the community. Continuous improvement efforts will help the CIE stay aligned with best practices and emerging trends in data governance and community information exchange.

Supporting the Technical Framework

The Technical and Operational Plan aims to create a technical foundation for the CIE by addressing the following areas:

- **Infrastructure Development:** Establishing a scalable and secure technical infrastructure capable of handling large-scale data integration and analysis. This includes the design and implementation of user-friendly interfaces, robust security measures, and scalable data integration services for the ongoing addition of new CIE partner organizations.

- **Data Interoperability:** Develop data models which ensure seamless data centralization from diverse systems through the development of standardized data formats, transformations, and interoperability protocols. This will facilitate efficient and accurate data sharing among partners.

- **Integrating Existing Partner Technologies:** Implementing the necessary technological change management to existing platforms while will support the transaction of data into and out of the CIE framework.

Data Sharing and Legal Framework

The Fresno CIE will be built upon a comprehensive data-sharing and legal framework designed to facilitate seamless, secure, and compliant exchange of information among participating entities. This framework is critical for ensuring that data sharing supports the CIE's objectives while safeguarding the privacy and rights of the individuals it serves.

Data Sharing

Key Principles

- **Transparency:** Clear and open communication about data sharing practices, ensuring all partners understand and agree to the terms of data exchange.
- **Inclusiveness:** Involving a diverse range of stakeholders in the development and implementation of data sharing practices to ensure they meet community needs.

- **Accountability:** Establishing mechanisms to hold all partners accountable for their role in data sharing, ensuring adherence to agreed-upon standards and protocols.

Data Integration and Centralization

- **Standardized Data Formats:** Using common data standards to ensure compatibility and interoperability across different systems, facilitating efficient data exchange.
- **Real-Time Data Sharing:** Implementing systems that enable the real-time transmission of critical information, such as suicide-related health data, to ensure timely interventions by partnering organizations.
- **Secure Data Handling:** Employing robust encryption and access control measures to protect data integrity and confidentiality during transmission and storage.

Legal

Compliance with Regulations

- **Data Privacy Laws:** Ensuring compliance with federal and state data privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA), to protect the privacy of individuals' health and personal information.
- **Consent and Authorization:** Establishing processes for obtaining informed consent and authorization for data sharing from individuals or their legal guardians, as required by law while ensuring an optimized service delivery model.

Monitoring and Enforcement

- **Regular Audits:** Conducting regular audits of data sharing practices and systems to ensure compliance with legal and regulatory requirements and to identify areas for improvement.
- **Continuous Improvement:** Implementing a process for continuous review and adaptation of data sharing and legal practices to keep pace with evolving legal standards and community needs.

Background

Partnership and Technical Discovery

From November 2023 to August 2024, a comprehensive review was conducted to assess the feasibility of developing a Community Information Exchange (CIE) in Fresno County. This discovery process encompassed extensive stakeholder engagement, the identification of pilot initiatives, the establishment of key success criteria, and the early definition of governance structures. Key activities included:

1. **Stakeholder Engagement:** Broad efforts were made to engage key stakeholders across various sectors, including healthcare, social services, education, and community organizations. More than 100 organizing sessions were convened, working with key stakeholder groups to organize implementation of the Fresno County CIE. This engagement was crucial for understanding the needs, expectations, and potential contributions of different partners.

2. **Identification of Pilot Initiatives:** Two pilot initiatives were identified to serve as the initial focus for the CIE development. These initiatives were chosen based on their potential impact, feasibility, and capacity to provide a solid framework from which to scale future work.

3. **Establishment of Success Criteria:** Key success criteria for early phases of the CIE development were established to guide the project and measure its progress. These criteria include technical feasibility, stakeholder participation, data integration capabilities, and improved service delivery outcomes.

4. **Early Definition of Governance:** An early governance framework was defined to ensure clear roles, responsibilities, and decision-making processes. This includes the development of a cross-sector CIE Core Team which drives operational and stakeholder engagement work.

5. **Selection of Partners:** Partners for the first phase of the CIE development were carefully selected based on their readiness, capabilities, and strategic alignment with the CIE's goals. These partners include healthcare providers, social services agencies, and educational institutions.

6. **Technical Interviews and Convening Workgroups:** Individual and group interviews were conducted with selected partners to gather detailed insights into their technical systems, data management practices, and collaborative potential. These interviews helped identify technical requirements and integration challenges, and were supported by convening CIE Workgroups.

7. **Development of the Technical and Operational Plan:** The findings from the discovery process and workgroups culminated in the development of the Fresno County CIE Technical and Operational Plan (TOP). The TOP provides a detailed roadmap for the implementation, management, and sustainability of the Fresno County CIE, outlining the necessary infrastructure, data workflows, governance structures, and operational procedures.

Through this thorough discovery process, the foundation has been laid for a successful and impactful CIE in Fresno County, aimed at enhancing service delivery and improving outcomes for the community.

Approaches to Pilot Implementation

Home Visitation

The Home Visitation pilot aims to improve the overall efficiency and impact of these vital services in Fresno County. In early phases of this pilot, four data systems will be interconnected to test the feasibility of interoperability and the impact of releasing new data to home visitation workers in the field. As data are updated between these partner systems, they will automatically feed to the CIE central hub, allowing for the seamless delivery of new and novel data into case records, which will enrich available data with the potential to optimize service delivery. Initial partners will include Fresno County Department of Public Health, Fresno County Department of Social Services, and Fresno County Superintendent of Schools.

Youth Suicide Prevention

The Youth Suicide Prevention pilot will be designed to test the initial technical and workflow feasibility of delivering real-time alerts to partner organizations which will initiate enhanced wrap around support for youth in critical need. Trigger data such as 5150 holds (involuntary admissions) will be securely delivered from participating healthcare partners to appropriate school district support staff and behavioral health experts. Initial partners include Fresno County Department of Behavioral Health, Central Unified School District, Sanger Unified School District, Manifest MedEx Health Information Exchange, and select Fresno County healthcare providers.

Partner Organizations and Roles

Home Visitation

Partner Overview: Fresno County Department of Public Health (FCDPH)

The Fresno County Department of Public Health (FCDPH) is dedicated to protecting and promoting the health and well-being of all Fresno County residents. The department provides a wide range of services aimed at improving public health outcomes, including immunizations, disease prevention and control, maternal and child health programs, environmental health services, and health education initiatives. FCDPH also plays a critical role in responding to public health emergencies and maintaining preparedness for natural and man-made disasters. Through its comprehensive public health programs and services, FCDPH strives to create a healthier, safer community for all residents.

The Fresno County Department of Public Health (FCDPH) is a pivotal partner in the Fresno County Community Information Exchange (CIE) Home Visitation Pilot. FCDPH contributes essential health data related to maternal and child health, immunizations, and developmental screenings. By integrating this data into the CIE, FCDPH enhances the unified case management system, facilitating coordinated care and timely interventions for families. The department also ensures compliance with stringent data privacy regulations, safeguarding the integrity and confidentiality of shared information. Through its involvement, FCDPH aims to improve health outcomes and support the well-being of children and families in Fresno County.

FCDPH Role in the Home Visitation Pilot

FCDPH is a pivotal partner in the CIE Home Visitation Pilot, providing the central technical and staffing assets to drive initial stages of the pilot. Home Visitation workers currently have limited access to key social services data, and the pilot will support enhanced access to case data related to the individuals they serve. Access to these enhanced case files will require workflow modifications for staff such as Public Health Nurses. The involvement of

FCDPH is crucial for ensuring the pilot's success, given its extensive experience and resources in Home Visitation services.

Responsibilities and Contributions (Proposed, subject to approval)

Data Integration and Sharing

- **Health Data Contribution:** FCDPH will contribute essential home visitation data related to maternal and child health, referrals, and developmental screenings. This data will be integrated into the CIE, allowing for more comprehensive case management and coordinated care.
- **Secure Data Sharing:** Ensuring that all health data shared is compliant with HIPAA and other relevant privacy regulations, FCDPH will employ security measures to protect the integrity and confidentiality of the information.

Monitoring and Evaluation

- **Outcome Tracking:** Monitoring home visitation outcomes and service utilization for individuals and families participating in the pilot. FCDPH will track key metrics determined by the Workgroup.
- **Feedback Loop:** Providing regular feedback to the CIE Core Team and Workgroups on the effectiveness of the pilot, identifying areas for improvement, and contributing to the continuous enhancement of the system.

Integration and Data Flow

The integration and data flow process for FCDPH involves several key steps:

- **Trigger Release of Health Data:** FCDPH will trigger the release of relevant health data from its electronic health record (EHR) systems and other data sources to maintain an up-to-date Master Person Index for matching against other data sources.
- **Channel Data to CIE:** Transmit the released data to the CIE's secure platform, ensuring that the data flow is timely, accurate, and compliant with all legal and regulatory requirements.
- **Data Matching:** The CIE will match FCDPH data against the existing directory, adding new records or assigning records in transit an existing Unique ID.
- **Import and Update Records:** The CIE will push updates from other data systems to the FCDPH data system, appending and enriching case records with data from other sources not native to the FCDPH system.

Partner Overview: Fresno County Department of Social Services

The Fresno County Department of Social Services (FCDSS) is committed to enhancing the quality of life for individuals and families in Fresno County by providing essential social services and support programs. FCDSS administers a variety of programs designed to assist those in need, including CalWORKs (California Work Opportunity and Responsibility to Kids), CalFresh (nutrition assistance), and Medi-Cal (healthcare coverage). The department also offers services related to child welfare, adult protective services, and employment assistance. Through these programs, FCDSS aims to promote self-sufficiency, protect vulnerable populations, and improve the overall well-being of the community.

FCDSS Role in the Home Visitation Pilot (Proposed, subject to approval)

FCDSS is considering how it may support early phases of the Home Visitation Pilot by providing workers in the field with enriched data such as Medi-Cal eligibility and access to services such as CalWORKS and CalFresh, improving the overall efficiency and effectiveness of Fresno’s homes visitation services. The involvement of FCDSS is vital for ensuring that home visitors have access to comprehensive social services data, empowering them to better serve families in need.

Potential Responsibilities and Contributions

Data Integration and Sharing

- **Social Services Data Contribution:** FCDSS can provide data from their locally hosted system which houses critical data from the California Statewide Automated Welfare System (CalSAWS) related to CalWORKs, CalFresh, and Medi-Cal. This information may be integrated into the CIE to facilitate a holistic understanding of a family's needs by partnering organizations and team members.
- **Secure Data Sharing:** Ensuring that all data shared is compliant with relevant privacy regulations, including safeguarding personally identifiable information (PII) and protected health information (PHI). FCDSS will offer robust security protocols to protect the integrity and confidentiality of the data.

Empowering Home Visitors

- **Enhanced Information Access:** Providing home visitors with access to detailed information about the families they serve, including their eligibility for and access to social services. This will enable home visitors to offer more informed and effective support.
- **Service Clarity:** Developing clarity around families' access to services and Medi-Cal eligibility, helping home visitors to guide families through the process of accessing benefits and support services.

Monitoring and Evaluation

- **Continuous Improvement:** Providing feedback to the CIE Core Team and Workgroups on the effectiveness of data integration and service delivery, identifying areas for improvement, and contributing to the ongoing enhancement of the system.

Integration and Data Flow

The integration and data flow process for FCDSS involves several key steps:

- **Capture Social Services Data:** FCDSS can capture relevant data from CalSAWS related to CalWORKs, CalFresh, and Medi-Cal within their local system. This data will provide insights into the socioeconomic status and needs of families.
- **Channel Data to CIE:** Transmit the triggered data to the CIE's secure platform, ensuring timely, accurate, and compliant data flow. This step is crucial for integrating social services information with other data sources within the CIE.
- **Data Matching and Case Management:** The CIE will match social services data against the panels of families enrolled in the home visitation programs. This matching process will help identify families who can benefit from coordinated services and interventions.
- **Triggering Alerts and Interventions:** When specific needs or eligibility issues are identified, the CIE can trigger alerts to relevant home visitors and case managers within FCDSS and partner organizations. These alerts will enable timely and targeted support for families.

Partner Overview: Fresno County Superintendent of Schools

The Fresno County Superintendent of Schools (FCSS) is dedicated to ensuring educational excellence and fostering academic success for all students in Fresno County. FCSS provides leadership, resources, and support to the county's public schools, working collaboratively with school districts to enhance educational programs and services. The office offers a wide range of services, including professional development for educators, special education support, curriculum development, and technology integration. FCSS also oversees various student programs aimed at improving academic achievement and preparing students for college and career readiness. Through its commitment to quality education, FCSS strives to empower students, educators, and communities to achieve their highest potential.

FCSS Role in the Home Visitation Pilot (Proposed, subject to approval)

FCSS will play a crucial role in testing the feasibility and efficacy of automating the delivery of reporting data from the Fresno County Department of Public Health (FCDPH) into their Apricot 360 data system, streamlining data management and improving service coordination.

Responsibilities and Contributions

Data Integration and Sharing

- **Automated Data Delivery:** FCSS will support the automation of reporting data from FCDPH regarding home visitation services. This data will be seamlessly integrated into the Apricot 360 data system used by FCSS, enhancing data accessibility and usability.
- **Secure Data Handling:** Ensuring that the data transfer process is secure and compliant with all relevant privacy regulations, protecting the integrity and confidentiality of sensitive information.

Enhancing Service Coordination

- **Data-Driven Decision Making:** Providing educators and service providers with access to data, allowing for more informed decision-making and targeted interventions to support the well-being of children and families.

Monitoring and Evaluation

- **Continuous Improvement:** Offering feedback to the CIE Core Team and Workgroups on the effectiveness of data integration and service coordination, helping to identify areas for improvement and contribute to the ongoing enhancement of the system.

Integration and Data Flow

The integration and data flow process for FCSS involves several key steps:

- **Capture Home Visitation Data:** FCDPH will capture detailed data on home visitation services, including health screenings, developmental assessments, and support provided to families.
- **Automate Data Transfer:** The CIE will automate the delivery of this data into FCSS' instance of the Apricot 360 data system, ensuring timely and accurate data integration. This process will minimize manual data entry and reduce the potential for errors, and test this automation process for future phases of development.

Youth Suicide Prevention

Partner Overview: Manifest MedEx (MX)

Manifest MedEx (MX) is a leading Health Information Exchange (HIE) in California, dedicated to improving healthcare outcomes through enhanced data sharing and collaboration among healthcare providers. MX provides a secure platform for exchanging health information, enabling providers to access critical patient data, improve care coordination, and enhance clinical decision-making.

MX Role in the Fresno CIE Youth Suicide Prevention Pilot

As a proposed backbone technology supporting early phases of the Fresno CIE Youth Suicide Prevention pilot, Manifest MedEx will play a crucial role in facilitating timely and actionable data sharing between healthcare, educational, and behavioral health partners. The primary responsibilities of MX in this pilot include:

- **Ingesting Diagnosis Code Data:** MX collaborates with healthcare partners to ingest data related to diagnosis codes such as T14.91 (suicide attempt and interrupted attempt); Z91.5 (personal history of suicide attempt(s); R45.851 (suicidal ideation) which serve as critical triggers for identifying at-risk youth in real-time.
- **Data Matching:** MX matches the trigger data against the panels of participating CIE partners. These panels are directories of individuals affiliated with the receiving organizations, such as students enrolled in a CIE Partner school district.

- **Transmitting Alerts:** When a match is identified, MX sends an alert to the relevant partner organization.

By leveraging its data integration and alerting capabilities, Manifest MedEx will enhance the ability of educational and behavioral health partners to respond quickly and effectively to potential suicide risks, thereby supporting the overall goal of the Youth Suicide Prevention pilot to safeguard and improve the mental health of school-age youth in Fresno County.

Healthcare Systems as Catchment for Trigger Data

The healthcare systems participating in development of the Fresno CIE Youth Suicide Prevention pilot will encompass a diverse array of hospitals and care centers throughout Fresno County. These institutions will play a pivotal role in capturing and channeling relevant diagnosis code data into Manifest MedEx's (MX) system in real-time. By integrating data from their respective Electronic Health Records (EHRs), these healthcare providers can ensure timely and accurate data flows, facilitating rapid response and intervention for at-risk youth.

Participating Healthcare Systems (Proposed)

- Clovis Community Medical Center - Clovis
- Community Regional Medical Center - Fresno
- Exodus Adult CSC
- Exodus Youth CSC
- Kaiser
- St. Agnes
- Reedley Adventist Health
- Coalinga
- Selma Adventist Health
- Valley Children's Hospital

Partner Overview: Sanger and Central Unified School Districts

Sanger Unified School District (SUSD) and Central Unified School District (CUSD) will play pivotal roles in early phases of development by receiving and acting upon real-time alerts related to at-risk students. These education partners have indicated a lack of real-time access to data on student behavioral health and support the development of CIE data integration to provide more comprehensive wraparound supports to students and their families in times of need.

The integration and data flow process for SUSD involves the following steps:

- **Panel Creation:** The districts will maintain a directory of students enrolled in the district. This directory, known as a panel, will be integrated with Manifest MedEx's (MX) system to enable data matching.
- **Receiving Alerts:** When a diagnosis code is captured and transmitted to MX by participating healthcare systems, MX will match the data against the district's student panel.
- **Alerts:** If a match is found, MX will transmit an alert to designated district staff.
- **Timely Interventions:** Upon receiving the alert, the districts can quickly identify the at-risk student and coordinate with appropriate educational and behavioral health resources to provide timely support and intervention, aiming to prevent potential crises and ensure the student's well-being.

By collaborating closely with MX and integrating into the CIE, these CIE partners enhance their ability to respond swiftly to mental health crises, thereby safeguarding the well-being of its students and contributing to the broader objectives of the Youth Suicide Prevention pilot.

Partner Overview: Fresno County Department of Behavioral Health

The Fresno County Department of Behavioral Health (FCDBH) is dedicated to providing comprehensive mental health and substance use disorder services to the residents of Fresno County. FCDBH offers a wide range of programs and resources aimed at improving the mental health and overall well-being of individuals and families. The department provides services across various settings, including outpatient clinics, residential treatment facilities, and community-based programs.

Members of the FCDBH team have highlighted the importance of effective communication among various agencies such as schools, behavioral health organizations, social services, and public health in supporting community needs. They noted that they currently lack a system to track the movement of the people they serve, particularly in relation to suicide prevention projects. Workgroup team members discussed the need for improvement in data management and communication systems to foster future collaboration and effective support for Fresno County residents.

Key Services and Programs

- **Mental Health Services:** FCDBH offers assessment, counseling, therapy, and psychiatric services for individuals experiencing mental health issues. This includes support for conditions such as depression, anxiety, bipolar disorder, and schizophrenia.
- **Substance Use Disorder Services:** The department provides treatment and recovery programs for individuals struggling with substance use disorders, including detoxification, residential treatment, and outpatient support.
- **Crisis Intervention:** FCDBH operates crisis intervention services, including a 24/7 crisis hotline, mobile crisis response teams, and emergency psychiatric services to support individuals in acute mental health crises.
- **Prevention and Early Intervention:** FCDBH focuses on prevention and early intervention programs designed to address mental health and substance use issues before they escalate. This includes educational outreach, community workshops, and early screening initiatives.
- **Support Services:** The department offers a range of support services, including case management, peer support, housing assistance, and vocational training to help individuals achieve stability and improve their quality of life.

FCDBH Role in the Youth Suicide Prevention Pilot

The Fresno County Department of Behavioral Health (FCDBH) is an important partner in the CIE Youth Suicide Prevention Pilot. As a recipient of alerts from Manifest MedEx (MX), FCDBH will play a significant role in responding to the immediate needs of children at risk of suicide or experiencing severe mental health crises. This partnership is essential for ensuring that timely and appropriate behavioral health interventions are provided to vulnerable youth.

Responsibilities and Contributions

Integration and Data Flow

The integration and data flow process for FCDBH involves several key steps:

- **Alert Reception:** FCDBH will receive real-time alerts from MX when a 5150 hold is placed on a youth. These alerts will be promptly delivered to designated staff members.
- **Data Utilization:** FCDBH will utilize the alert information, along with any additional data provided, to assess the situation and determine the most appropriate response. This may include coordinating with other service providers to ensure a holistic approach to care.
- **Coordinated Care:** Ensuring that all relevant information is shared with necessary team members and partners to facilitate a coordinated response. This ensures that all parties involved have the

information needed to provide effective support and intervention.

Overview of Data Systems and Platforms

Home Visitation

Overview

There are a broad array of case management and other data systems in use across Fresno County's home visitation landscape. Early phases of CIE development will integrate a representative and high-impact sample of these systems to develop the foundation for universal case management, which will include myAvatar and CCS Community Health Record System, managed by the Department of Public Health; CalSAWS (by way of a locally hosted instance of Data Service), managed by Department of Social Services; and Apricot 360, managed by the Fresno County Superintendent of Schools.

myAvatar

myAvatar is an enterprise electronic health records system currently in use by the Fresno Department of Public Health (DPH) for case management, reporting, and as a staging area for delivering mandatory reporting to other data systems. It is the central clearing house for all home visitation data managed by DPH.

> **Considerations for CIE Integration**: Fresno County's instance of myAvatar is hosted on premises by the Department of Public Health and does not have an active API gateway, which limits its use for incorporation into the CIE platform without technical rework. There several options for development of this integration gateway described within the technical sections of the TOP.

Fresno Department of Social Services Data Systems

The Fresno Department of Social Services (DSS) manages local databases with a suite of tools, technologies, and applications designed to help organizations collect, analyze and present business data. It encompasses a range of products that enables users to gather, process and visualize data from various sources. Amongst other use cases, DSS uses their data systems to push and pull data from the California Statewide Automated Welfare System (CalSAWS).

CalSAWS is a case management system providing CalWORKs, CalFresh, Medi-Cal, Foster Care, Refugee Assistance, County Medical Services Program, and General Assistance/General Relief to children, families, and individuals across all California counties. It encompasses the following functions: eligibility determination, benefits calculation, benefits issuance, and information management.

> **Considerations for CIE Integration**: DSS has a robust set of tools for data integration but will require engagement and approval from senior leadership for their use.

Apricot 360 (Bonterra Impact Management)

Apricot 360 is an enterprise system designed for small to mid-sized nonprofit organizations. Apricot software is an all-in-one platform that is built around the ability to allow organizations to self-define and customize their datasets, reporting, and dashboards to best suit their organization's mission. The Apricot platform is in use by multiple home visitation programs across Fresno County.

Considerations for CIE Integration: The high degree of customization between each instance of the Apricot platform deployed in Fresno County will require either agreement among CIE partners to adhere to strict data standards or for the CIE system to accommodate customized data transformations. Apricot 360 is not capable of making or answering API calls on its own, and instead relies on 3rd-party systems such as Workato or Zapier. Integration of any local Apricot instance into the CIE will require the addition of these 3rd-party API services.

CCS Community Health Record (CHR) System

The CHR is an EHR developed with data interoperability as a key central component. Key functionalities of the product are focused on providing a complete view of a client's information at all stages of engagement in order maximize the positive outcome for the individual. Fresno Department of Public Health has 150 end users and more than 2000 clients in the system with relatively low levels of traffic.

Considerations for CIE Integration: CHR is designed for seamless integration into existing data systems. As a 3rd-party product, legal agreements will be needed for its incorporation into the CIE which may involve revisions to existing contracts.

Youth Suicide Prevention

Overview

Suicide prevention is a complex and multifactor issue with a number of existing initiatives operating within the Fresno County landscape. Early phases of the CIE will focus on developing a streamlined early-alert system designed to send confidential messages to recipient organizations when a diagnosis code is entered into participating healthcare organizations' electronic health record systems. This pilot system will integrate diagnosis code data from existing healthcare system EHRs in the Manifest MedEx platform, match these data against panels submitted by partners receiving alerts, and submit a alert to the receiving partner. There are multiple existing data systems operating within this current ecosystem.

Manifest MedEx Health Information Exchange

Manifest MedEx (MX) is a comprehensive health information exchange (HIE) system designed to facilitate the seamless and secure sharing of healthcare data among various stakeholders, including hospitals, clinics, and public health organizations. The system integrates and aggregates patient data from multiple sources, providing a centralized platform for real-time access to medical records, lab results, and care coordination information. MX employs advanced data security and privacy measures to ensure compliance with regulatory standards and protect patient confidentiality. By offering interoperability features and analytics capabilities, MX enhances clinical decision-making, improves patient outcomes, and supports public health initiatives.

Considerations for CIE Integration: The MX data system provides proven technologies for the ingestion, integration, and delivery of electronic health records. These capabilities will need to be assessed for ingestion, integration, and management of FERPA-protected student records, resulting in the potential for revision of practices and technical approach to data management.

Sanger Unified: PowerSchool

PowerSchool is a leading student information system (SIS) widely used by educational institutions to manage and streamline various administrative tasks and student data. PowerSchool provides a comprehensive platform that integrates student records, attendance, grades, and other essential information, facilitating efficient data management and improving educational outcomes.

Considerations for CIE Integration: While PowerSchool offers a wide array of data integration capabilities, SUSD team members will need to configure the system to meet their internal administrative requirements and to satisfy the agreed-upon needs of the CIE partnership, such as the frequency of panel updates and the ingestion of key data fields.

Central Unified: Aeries Student Information System

Aeries Student Information System (SIS) is a comprehensive and user-friendly platform designed to manage and streamline student data for K-12 educational institutions. It offers a wide range of features, including student enrollment, attendance tracking, grade reporting, and assessment management. Aeries SIS supports seamless communication between teachers, administrators, parents, and students through its integrated portals, enhancing engagement and collaboration. The system's robust reporting and analytics tools enable educators to monitor student performance, identify trends, and make data-driven decisions to improve educational outcomes. With its emphasis on data security and compliance, Aeries SIS ensures the confidentiality and integrity of student information, making it a trusted solution for schools seeking to enhance their administrative efficiency and educational effectiveness.

Considerations for CIE Integration: While Aries offers a wide array of data integration capabilities, CUSD team members will need to configure the system to meet their internal administrative requirements and to satisfy the agreed-upon needs of the CIE partnership, such as the frequency of panel updates and the ingestion of key data fields.

Smart Care

SmartCare EHR is a comprehensive electronic health record system designed to support behavioral health and human services organizations. This advanced platform facilitates the seamless management of patient information, including clinical documentation, treatment plans, medication management, and appointment scheduling. SmartCare EHR is tailored to meet the unique needs of behavioral health providers, offering specialized features such as progress notes, care coordination, and outcome tracking. With robust interoperability capabilities, SmartCare EHR ensures secure data sharing across various healthcare settings, enhancing care continuity and collaboration among providers. Additionally, its intuitive interface and customizable workflows improve efficiency and usability for clinicians, ultimately contributing to better patient outcomes and streamlined administrative processes.

Considerations for CIE Integration: The Smart Care system has not been assessed for technical integration into the CIE.

Electronic Health Record Systems

There are a variety of Electronic Health Record Systems (EHRs) in use by healthcare organizations. Electronic Health Records (EHRs) are digital versions of patients' paper charts used within healthcare systems to streamline the management and sharing of patient information. EHR systems capture comprehensive patient data, including medical histories, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory test results. By providing real-time, patient-centered records accessible to authorized healthcare providers, EHRs facilitate coordinated and efficient care delivery. Key EHR systems used within healthcare include Epic, Cerner, Allscripts, and Meditech, each offering robust features for clinical documentation, order entry, decision support, and reporting. These systems enhance the quality of care, improve patient outcomes, and ensure compliance with regulatory standards, all while maintaining the security and confidentiality of sensitive patient information.

Considerations for CIE Integration: EHR systems have mandatory integration capabilities. The method of 5150 hold delivery will rest on the internal requirements of the various healthcare partners and agreed-upon standards set with MX.

Impact of Legislation on CIE Development

California's AB 133 Bill

California Assembly Bill 133, enacted in 2021, is a comprehensive health care legislation aimed at improving the state's health care delivery and data infrastructure. Key components of AB 133 include:

1. **Health Data Sharing and Exchange:** Mandating the establishment of a statewide health information exchange (HIE) network to facilitate the secure sharing of health data among providers, payers, and patients.
2. **Data Exchange Framework:** Requiring the development of a standardized data exchange framework to ensure interoperability among various health IT systems.
3. **CalAIM (California Advancing and Innovating Medi-Cal) Initiatives:** Supporting the integration of Medi-Cal services with broader health and social services, promoting whole-person care.
4. **Equity and Access:** Focusing on health equity by improving access to quality care for underserved and vulnerable populations through better data collection and analysis.

Impact on Community Information Exchanges in California

The implementation of AB 133 is poised to significantly enhance the landscape for community information exchanges (CIEs) in California in several ways:

1. **Enhanced Interoperability:** The standardized data exchange framework mandated by AB 133 will improve the interoperability between CIEs and other health IT systems, enabling

seamless sharing of health and social service data across different organizations and platforms.

2. **Increased Data Integration:** By promoting the integration of health, social, and Medi-Cal services, AB 133 will enable CIEs to provide more comprehensive and coordinated care. This integration will facilitate a holistic approach to addressing the needs of individuals, particularly those from underserved communities.
3. **Improved Data Accessibility:** The establishment of a statewide HIE network will ensure that data collected by CIEs is more readily accessible to health care providers, payers, and patients. This accessibility will lead to better-informed decision-making and more effective interventions.
4. **Focus on Health Equity:** AB 133's emphasis on health equity and improved access to care for vulnerable populations will empower CIEs to better serve these communities by leveraging enhanced data capabilities to identify and address disparities in health outcomes.
5. **Support for Whole-Person Care:** The alignment with CalAIM initiatives will encourage CIEs to adopt a whole-person care approach, integrating physical health, behavioral health, and social services to provide comprehensive support for individuals' overall well-being.

Overall, AB 133 is expected to strengthen the role of community information exchanges in California, enabling them to play a critical part in the state's efforts to improve health outcomes and promote health equity.

California Senate Bill (SB) 929: Overview and Impact on 5150 Hold Data for Suicide Prevention

SB 929, introduced in February 2022 and in effect on January 1, 2023,, focuses on expanding the state's response to mental health crises, including refining the protocols for involuntary psychiatric holds under section 5150 of the California Welfare and Institutions Code. A "5150 Hold" allows individuals experiencing a mental health crisis and posing a danger to themselves or others to be held involuntarily for up to 72 hours for assessment, evaluation, and crisis intervention.

SB 929 aims to improve transparency, data collection, and coordination across state and local agencies, with an emphasis on mental health outcomes. It seeks to enhance how agencies collect and share data related to mental health holds, crisis services, and psychiatric care, and to ensure that data can be used to inform policy, prevention efforts, and care coordination.

Impact on Fresno CIE's Suicide Prevention Pilot

The Fresno Community Information Exchange (CIE) is exploring the use of data from 5150 holds to inform a suicide prevention pilot, aiming to better identify and support individuals at risk. SB 929 presents several key opportunities for leveraging 5150 hold data:

1. **Improved Data Access and Sharing:** SB 929 supports the sharing of 5150 hold data between health and community-based organizations while ensuring privacy protections. This creates an opportunity for the Fresno CIE to access more comprehensive data on individuals in crisis and integrate it into the CIE system, improving care coordination and timely interventions for those at risk of suicide.

2. **Enhanced Coordination Across Systems:** The bill encourages collaboration between mental health agencies, hospitals, law enforcement, and community-based organizations. Fresno CIE can use this coordination to establish partnerships with stakeholders that handle 5150 holds, allowing them to identify high-risk individuals and provide appropriate support through the CIE platform.
3. **Ethical Data Use for Prevention:** While SB 929 facilitates better data sharing, it also reinforces strict privacy and ethical guidelines. For the Fresno CIE, this means using 5150 hold data responsibly, ensuring consent where appropriate, and using aggregated or de-identified data for prevention purposes, reducing suicide risk in a manner compliant with California's privacy laws.
4. **Pilot for Early Intervention:** With enhanced data access, the Fresno CIE can identify patterns or trends in 5150 holds that signal a heightened suicide risk, enabling early intervention and outreach as part of the suicide prevention pilot. This can lead to more proactive, targeted support for individuals before they experience another crisis.

In summary, SB 929 enhances Fresno CIE's ability to use 5150 hold data ethically and effectively for suicide prevention, enabling the pilot program to provide timely support and coordination of care for individuals in crisis.

Conclusion

This thorough understanding of the Fresno County community ecosystem, as it relates to developing a CIE, enables the partnership to address the unique needs and challenges of diverse stakeholder community, ensuring that the CIE is poised to deliver significant improvements in data sharing, service coordination, and ultimately, community health outcomes. As we move forward with the implementation of the CIE, this background will serve as a critical reference point, guiding our technical and operational decisions and ensuring alignment with our overarching mission and goals.

Technical & Operational Plan

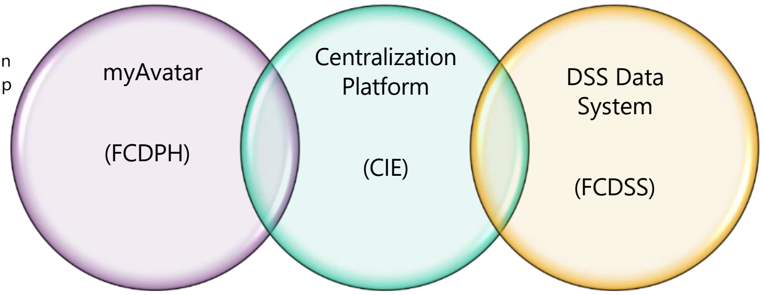
This section outlines proposed technical architecture, operational processes, governance structures, and legal frameworks that will support the effective integration and management of data across various participating organizations. By establishing clear guidelines and protocols, the TOP ensures that the CIE operates securely and efficiently, ensuring a high likelihood of success for Phases 1 and 2 of CIE development and enhancing the prospect of improved service delivery and outcomes for the residents of Fresno County.

Plan Overview

To meet the requirements for Fresno CIE in achieving key results for the children and families of Fresno County, the Technical and Operational Plan takes a data centralization perspective (see Figure 1). This data centralization concept is designed with the following high-level approach:

1. Existing primary data Systems of Origin for the CIE partners will need approval for release of data for integrate into the CIE Framework and permanent storage and use by the third-party data system vendor.
2. A standalone integration system (CIE) will be developed to support and facilitate information centralization from these primary systems.
3. System governance will need to be developed, maintained, and evolved by the CIE partners to ensure the Fresno CIE continues to drive effective and secure utilization of the common platform.

- Household Information
- Referrals and follow-up
- Case Management
- Location



- Medi-Cal
- CalFresh
- CalWORKS

Enabling Functionality for:

- Enriched Case Files
- Ongoing System Integration
- Provider Communications

Figure 1: Centralized Data Exchange Example Diagram

System Features, Requirements and Considerations

Development of the Integrating System will require the features, requirements, and considerations below:

Technical and Operational Plan Considerations

	Features, Requirements, and Considerations
Data Management	• Data segregation • Agreements needed: Service Level Agreements (SLAs), Data Sharing Agreements (DSAs), etc. • Scalability
Data Security	• Disclosure • Data Backup • Data Archiving for Security • Disposal of Data • Location Security • Redundant Utilities • Data Encryption (at rest and in transit)
Data Retention	• Statutory and policy/practices concerning length of time different types of information (including PII and PHI) is retained by various entities
Data Flow	• Determine data endpoints and how they are to connect • Entities providing input and output data • High-level preliminary Data Flow
Data Access & Permissions	• Configurable role-based access & permissions • Single sign on (SSO) supportability and integration • Authentication (Multi-Factor) and Authorization
Privacy & Protocols	• Audit Trail History • Automated Privacy Monitoring • Protocols to be defined with consideration to: ○ Health Insurance Portability and Accountability Act (HIPAA) and 42 Code of Federal Regulations Part 2 (42 CFR Part 2) and exceptions in the event of a medical emergency ○ Uniform Health Care Information Act (UHCIA), RCW 70.02 ○ RCW 39.26.340, which requires DSAs for Cat 3 or higher data (NOTE: this has cybersecurity implications as well as privacy and is related to Engrossed Substitute Senate Bill 5432 (ESSB 5432) implementation) ○ Health Information Technology for Economic and Clinical Health (HITECH) ○ Patient, client, or parent consent (when required)
Cybersecurity	• Ensure compliance with federal and state laws • Alignment with any rules deemed by the office of cybersecurity in consideration of ESSB 5432
Integration or Interoperability	• Integration with Partner System of Origin • Application Programming Interfaces (APIs), API management & Integration • Use of established data standards for data exchanges whenever able
Data Analytics & Performance Metrics	• Key Performance Indicators (e.g., Number of Families Engaged; Number of On-time Referrals, Linkage Rates, etc.) • Referral System Performance Indicators (e.g., Family was referred to follow-up services; Family received follow-up services (e.g., received referral appointment within 24 hours), Follow-up with family completed and outcomes documented) • Custom reporting and dashboards
Hosting Platform	• Cloud-hosted Platform-as-a-Service (PaaS) where feasible • Ability to connect to both cloud-based and on-premises systems

Solution Architecture	• Microservices based architecture when possible • Use APIs to move data between services when possible • Use flat files to move data only when necessary • Data architecture that aligns with industry best practices and is scalable, enables data analytics and reporting systems that support real-time monitoring data visualization capabilities • An integration architecture that meets industry standards for security and data exchange and enables secure, interoperable information exchange of PII and PHI
Liability	• Liability types • Liability management and mitigation

Data Management

The Technical and Operational Plan will reflect the goals and interests of a Fresno CIE Steering Committee or similar presiding decisioning body as it is developed through the Governance Framework. In addition, it will address a variety of data management issues including: what are the systems, users, storage, security, and documentation needs; and how to ensure data quality and appropriate permissions for data access (particularly given the sensitive nature of this data). The final data management plan will consider the many actors and entities who are unique yet interdependent, and the specific data elements that need to be shared while ensuring data can be appropriately protected and segregated. Activities that will be undertaken to define needed data management requirements include identifying:

- Data to be transmitted and accessed for different purposes (e.g., support referrals and coordination in care) and the system users for these purposes
- Data transmission and exchange protocols
- How data will be integrated (matching algorithm, cross system UUID and Master Person Index development, etc.)
- API's need for integration and API management technology
- Data segregation and segmentation based primarily on:
  - data type
  - sensitivity associated with the type of data
  - type of entry source for future integration considerations
- Identified custom reports and dashboards

Data Security

All data integration solutions will be required to include at a minimum information on:

- Disclosure Policies and Procedures
- Data Backup
- Data Archiving for Security
- Disposal of Data
- Location Security
- Redundant Utilities
- Encryption (at rest and in transit)

Ensuring industry-standard data security is crucial for the integrity and trustworthiness of the Fresno County CIE. All data integration solutions utilized within the CIE must meet stringent security requirements to protect sensitive information and maintain compliance with relevant standards. The following outlines the minimum required components for data security in the CIE.

Disclosure Policies and Procedures

- **Clear Protocols:** Establish and document clear protocols for the disclosure of data, detailing who has access to what information and under what circumstances data can be shared.
- **Consent Management:** When needed, ensure that all disclosures comply with consent agreements from data subjects, including provisions for parental or guardian consent where applicable.
- **Incident Reporting:** Implement procedures for promptly reporting any unauthorized disclosures or breaches, including notification to affected parties and regulatory bodies as required by law.

Data Backup

- **Regular Backups:** Conduct regular backups of all critical data to secure locations, ensuring that data can be restored in the event of loss or corruption.
- **Backup Verification:** Implement processes for regularly testing and verifying backups to ensure data integrity and reliability.
- **Offsite Storage:** Store backups in offsite locations to protect against physical damage to primary data centers.

Data Archiving for Security

- **Secure Archiving:** Archive data securely to protect it from unauthorized access and tampering. Archived data should be encrypted and stored in compliance with regulatory requirements.
- **Retention Policies:** Establish clear data retention policies that specify how long data must be archived and the conditions under which it can be accessed or restored.

Disposal of Data

- **Secure Disposal Methods:** Implement secure disposal methods for data that is no longer needed, ensuring that it is irretrievably destroyed. This includes both digital data and physical records.
- **Documentation:** Maintain documentation of data disposal processes, including records of what data was disposed of, when, and by whom.

Location Security

- **Physical Security Controls:** Ensure that data centers and storage locations are secured with physical controls such as biometric access, surveillance cameras, and security personnel.
- **Access Controls:** Implement strict access controls to limit physical access to authorized personnel only. Regular audits should be conducted to ensure compliance.

Redundant Utilities

- **Power Redundancy:** Ensure that data centers have redundant power supplies, including uninterruptible power supplies (UPS) and backup generators, to maintain operations during power outages.
- **Network Redundancy:** Implement redundant network connections to ensure continuous data flow and access even if one connection fails.
- **Cooling and Environmental Controls:** Use redundant cooling systems and environmental controls to protect hardware from overheating and other environmental hazards.

Encryption

- **Encryption at Rest:** Encrypt all data stored within the CIE to protect it from unauthorized access and breaches. This includes databases, file systems, and backups.
- **Encryption in Transit:** Encrypt data transmitted across networks using secure protocols such as TLS/SSL

to protect it from interception and tampering.

- **Key Management:** Implement key management practices to ensure that encryption keys are stored securely and rotated regularly to maintain data security.

By adhering to these comprehensive data security measures, the Fresno County CIE can ensure the protection of sensitive information, maintain compliance with regulatory standards, and uphold the trust of all stakeholders. These protocols provide a solid foundation for secure data integration and management, essential for the effective and reliable operation of the CIE.

Data Retention

Effective data retention policies are crucial for the management, security, and compliance of the Fresno County CIE. These policies ensure that data is retained for the appropriate duration, securely stored, and properly disposed of when no longer needed. The following outlines the key components of the data retention policies for the CIE.

Purpose and Scope

The data retention policies for the CIE aim to:

- Ensure compliance with legal, regulatory, and organizational requirements.
- Protect sensitive and personal information.
- Support the operational needs of the CIE.
- Facilitate data management and storage efficiency.

These policies apply to all data collected, processed, stored, and shared within the CIE, including health records, social services data, educational information, and any other personal or sensitive data.

Data Retention Periods

- **Legal and Regulatory Compliance:** Retain data for the period required by applicable laws and regulations, including HIPAA, FERPA, and state-specific regulations.
- **Operational Needs:** Retain data as long as necessary to support the operational and analytical needs of the CIE and its participating organizations.
- **Archival Data:** Certain data may be archived for historical analysis and research purposes, subject to anonymization and compliance with privacy regulations.

Data Storage and Security

- **Secure Storage:** All data must be stored in secure, access-controlled environments. Encryption must be used to protect data at rest.
- **Access Controls:** Implement role-based access controls to ensure that only authorized personnel can access sensitive data.
- **Regular Audits:** Conduct regular audits of data storage practices to ensure compliance with retention policies and security standards.

Data Disposal

- **Secure Disposal Methods:** Implement secure disposal methods for data that is no longer required. This includes:
  - Digital Data: Use secure deletion tools to permanently erase digital data.
  - Physical Records: Shred or incinerate physical records to prevent reconstruction.
- **Documentation:** Maintain records of data disposal activities, including the type of data disposed of, the disposal method used, and the date and personnel involved in the disposal.

Data Retention Reviews

- **Regular Reviews:** Conduct regular reviews of data retention practices and policies to ensure they remain aligned with legal requirements and organizational needs.
- **Policy Updates:** Update data retention policies as necessary to reflect changes in laws, regulations, or operational requirements.

Compliance and Accountability

- **Responsibility:** Designate specific personnel or teams responsible for overseeing data retention practices and ensuring compliance with these policies.
- **Training and Awareness:** Provide regular training to all CIE participants on data retention policies, secure data handling practices, and compliance requirements.
- **Incident Management:** Implement procedures for managing and responding to incidents related to data retention, including unauthorized data retention or disposal.

Special Considerations

- **Legal Holds:** In the event of litigation or legal investigations, suspend normal data disposal processes and retain relevant data until the legal hold is lifted.
- **Parental or Guardian Consent:** Ensure that data retention practices involving minors comply with applicable consent requirements and privacy protections.

The data retention policies of the Fresno County CIE are designed to ensure that data is managed responsibly, securely, and in compliance with all relevant laws and regulations. By adhering to these policies, the CIE can maintain the integrity, confidentiality, and availability of data, supporting the needs of its stakeholders while protecting the privacy and rights of individuals.

Data Access and Permissions

The CIE will require robust role-based access control. Data must be accessible to engage and/or refer children and families on a need-to-know basis only and in accordance with federal and state law. Policies, procedures, training, and compliance will be an integral part of maintaining the privacy and security of the technology systems and platforms.

The following table includes examples of some of the potential roles that could be required for accessing and using CIE. Each use case and each system integrated into the CIE will be evaluated individually and treated separately during the development phase.

Sample Roles and Permissions – High Level

Role	Description	Some Possible Permissions & Data Access
System Administrator/ Security Administrator/ Business Analyst	Role applied to users requiring full access to analytics, reporting, users, quality assurance portals, etc.	• Full control of reporting & analytics • User management access (add/delete users, assign any role or data restriction). • Ability to grant administrator permissions to users • Read/Write/Delete permissions

Program Manager or similar role	Role applied to registered providers of data	• Access to programmatic data to understand performance of program
Policy Makers	Decision-makers that only need access to aggregated data visualizations with no risk of exposing PII or PHI	• Access to high-level visualizations
Individual	Public-facing data	• Access to public-facing website
County Authorized Representatives	Job Specialists	• Access to send and/or view referrals and check for status updates

Privacy & Protocols

Ensuring the privacy and security of data within the Fresno County CIE is paramount. This section outlines the key privacy considerations and protocols that govern the handling, sharing, and protection of sensitive information within the CIE. By adhering to these standards, the CIE aims to maintain the highest levels of trust, compliance, and data integrity.

Key Privacy Principles

1. **Confidentiality:** Ensure that all personal and sensitive information is accessible only to authorized individuals and organizations. This includes implementing robust access controls and encryption protocols.
2. **Integrity:** Maintain the accuracy and consistency of data throughout its lifecycle. This involves regular audits, validation checks, and error handling mechanisms to prevent unauthorized alterations.
3. **Availability:** Guarantee that data is accessible to authorized users when needed. This involves implementing redundancy, backup solutions, and disaster recovery plans.
4. **Transparency:** Provide clear and comprehensive information to all stakeholders about how their data is being used, shared, and protected. This includes detailed privacy notices and regular updates on data practices.

Data Handling Protocols

1. **Data Collection:**
    - Collect only the minimum necessary data required for the specific purpose.
    - Ensure data collection methods comply with relevant legal and regulatory requirements.
2. **Data Storage:**
    - Store data in secure, access-controlled environments.
    - Use encryption to protect data at rest and in transit.
3. **Data Access:**
    - Implement role-based access controls to restrict data access to authorized personnel only.
    - Use multi-factor authentication to enhance security for accessing sensitive data.
4. **Data Sharing:**
    - Share data only with authorized partners and for specific, predefined purposes.
    - Ensure that data sharing agreements are in place with all partners, outlining the terms and conditions of data use.
5. **Data Retention and Disposal:**
    - Retain data only for as long as necessary to fulfill its intended purpose.
    - Implement secure disposal methods to ensure that data is irretrievably deleted when no longer needed.

Compliance with Legal and Regulatory Standards

1. **HIPAA Compliance:**
   - Ensure all data handling practices comply with the Health Insurance Portability and Accountability Act (HIPAA) to protect health information.
2. **FERPA Compliance:**
   - Adhere to the Family Educational Rights and Privacy Act (FERPA) regulations to protect educational records.
3. **State and Local Regulations:**
   - Comply with California state privacy laws and any local regulations governing data privacy and security.
4. **Welfare Institution Codes (WIC):**
   - Applicable data must follow review and validation guidelines as set by WIC

Incident Response and Management

1. **Incident Detection:**
   - Implement systems for continuous monitoring to detect potential data breaches or security incidents promptly.
2. **Incident Response Plan:**
   - Develop and maintain an incident response plan that outlines the steps to be taken in the event of a data breach or security incident.
3. **Notification Procedures:**
   - Establish procedures for notifying affected individuals and relevant authorities in the event of a data breach, in compliance with legal requirements.
4. **Post-Incident Analysis:**
   - Conduct a thorough analysis of any security incidents to identify root causes and implement measures to prevent future occurrences.
5. **Incident Reporting**:
   - Potential to offer capabilities for end-users to create/submit incidents and communicate resolutions (such as discrepancies, data errors, etc.)

Training and Awareness

1. **Regular Training:**
   - Provide regular training to all CIE participants on data privacy, security protocols, and best practices.
2. **Awareness Programs:**
   - Conduct ongoing awareness programs to keep all stakeholders informed about the importance of data privacy and the measures in place to protect it.

Cybersecurity

Ensuring robust cybersecurity measures is critical to the success and integrity of the Fresno County Community Information Exchange (CIE). Any third-party technology solutions integrated into the CIE must comprehensively address and manage several key areas of cybersecurity to protect the sensitive data and ensure the system's resilience against potential threats. Below are the essential components of the cybersecurity framework that must be implemented:

Physical and Environmental Protections

- **Data Centers:** Data centers must have stringent physical security measures, including access controls, surveillance systems, and security personnel, to prevent unauthorized physical access.

- **Environmental Controls:** Implement environmental controls to protect hardware from natural disasters, fires, and other environmental hazards, including climate control, fire suppression systems, and flood prevention measures.

Data Security

- **Encryption:** Employ strong encryption protocols for data at rest and in transit to protect sensitive information from unauthorized access and breaches.
- **Data Integrity:** Implement mechanisms to ensure data integrity, such as checksums and digital signatures, to detect any unauthorized alterations to data.
- **Backup and Recovery:** Maintain regular data backups and establish robust data recovery procedures to ensure data can be restored in the event of a loss or breach.

Network Security

- **Firewalls:** Use advanced firewall technologies to monitor and control incoming and outgoing network traffic based on predetermined security rules.
- **Intrusion Detection and Prevention Systems (IDPS):** Deploy IDPS to detect and prevent potential security breaches and attacks on the network.
- **Virtual Private Networks (VPNs):** Use VPNs to secure remote access to the CIE network, ensuring encrypted connections and protecting data during transmission.

Access Security

- **Authentication:** Implement multi-factor authentication (MFA) to verify the identities of users accessing the system.
- **Authorization:** Enforce strict access controls and role-based access management to ensure users only have access to the data and systems necessary for their roles.
- **User Activity Monitoring:** Monitor and log user activities to detect and respond to suspicious behavior and unauthorized access attempts.

Application Security

- **Secure Development Practices:** Follow secure coding practices and conduct regular code reviews and vulnerability assessments to identify and mitigate security risks in application development.
- **Patch Management:** Regularly update and patch applications to protect against known vulnerabilities and security threats.
- **Application Firewalls:** Implement web application firewalls (WAF) to protect applications from common web-based attacks, such as SQL injection and cross-site scripting (XSS).

Operations Management

- **Security Policies and Procedures:** Develop and enforce comprehensive security policies and procedures to guide all aspects of operations management.
- **Access Audits:** Conduct regular audits of access controls and security policies to ensure compliance and identify areas for improvement.
- **Training and Awareness:** Provide ongoing cybersecurity training and awareness programs for all personnel to ensure they understand and adhere to security best practices.

Security Monitoring and Logging

- **Continuous Monitoring:** Implement continuous security monitoring to detect and respond to security events in real time.

- **Centralized Logging:** Use centralized logging systems to collect, analyze, and store logs from various sources, providing a comprehensive view of security activities.
- **Anomaly Detection:** Employ advanced analytics and machine learning to detect anomalies and potential security incidents from log data.

Incident Response

- **Incident Response Plan:** Develop a detailed incident response plan outlining the procedures for identifying, managing, and mitigating security incidents.
- **Incident Response Team:** Establish a dedicated incident response team trained to handle and respond to security breaches effectively.
- **Post-Incident Analysis:** Conduct thorough post-incident analysis to understand the root cause of security incidents and implement measures to prevent future occurrences.

By addressing these key areas, third-party technology solutions can provide a cybersecurity framework that safeguards the Fresno County CIE, ensuring the protection of sensitive data and the continued trust of all participating organizations and stakeholders.

Partner Requirements Documentation

To participate in the Community Information Exchange (CIE), partners must meet certain system functionality requirements. The following outlines the minimum and preferred system requirements for partners to effectively connect to and utilize the CIE.

Minimum Viable System Requirements

1. Data Exports

- **Partial Data Exports:**
  - Capability to export only the rows within a database that have been created or updated within a specified time period.
  - The exports should contain only the data required by the CIE's common dataset.
  - Ability to export only the fields within a record that have been changed or updated.
- **Data Formatting:**
  - Exported data must be formatted according to CIE data definitions.
  - If the export process is manual, the partner must agree to upload the data on a consistent, agreed-upon schedule.
- **File Format:** Data should be exported in a flat file, CSV format.

3. Agreement to Common Partner SLA

- Partners must agree to a common understanding for maintaining their connection to the CIE. This includes being responsible for supplying crucial information to other partners in a timely and reliable form, signifying a social contract.

Preferred System Requirements

1. Data Exports

- **Triggered Exports:**
  - Ability to trigger data exports upon record save.
  - Exported data must be formatted according to CIE data definitions.
- **API Calls:**
  - Capability to make external HTTPS API calls to third-party endpoints with the payload from the

record save.

  - For new records, include the entirety of the record that maps to the CIE dataset.
  - For updates, include only the updated fields within the record that map to the CIE dataset.

2. Agreement to Common Partner SLA

- Partners must agree to a common Service Level Agreement (SLA) to maintain their connection to the CIE. This includes being responsible for supplying crucial information to other partners, signifying a social contract.

By adhering to these system requirements, partners can ensure seamless integration with the CIE, facilitating efficient data sharing and management. These requirements help maintain data integrity, consistency, and reliability across the CIE, supporting the collaborative goals of the participating organizations.

Fuzzy Matching System Evaluation Requirements

To ensure that the CIE can effectively match and integrate data from diverse sources, it is crucial to evaluate the capabilities of fuzzy matching systems thoroughly. The following criteria outline the key requirements for an effective fuzzy matching system, taking into consideration various name variant phenomena, global name ethnicity specifics, entity types, and other critical factors.

1. Handling a Variety of Name Variant Phenomena

- **Misspelling:** Can the system identify and match names with common misspellings? (e.g., John Richards vs. John Richarda)
- **Names with the Same Sound:** Can it recognize phonetic variations of names? (e.g., Kay vs. Kaye; Allen vs. Allan vs. Alan)
- **Nicknames:** Does it handle common nicknames and their formal counterparts? (e.g., Robert vs. Bob vs. Bobby; Theodore vs. Ted)
- **Initials:** Can it match names with initials? (e.g., John Ronald Smith vs. J. R. Smith)
- **Name Order Variants:** Can it recognize names with reversed order? (e.g., Fumio Kishida vs. Kishida Fumio)
- **Missing Name Elements:** Can it match names with missing elements? (e.g., John Frank Robertson vs. John Robertson)
- **Company Abbreviations:** Does it handle abbreviations of company names? (e.g., Bayerische Motoren Werke AG vs. BMW; Smith, Jones, & Company LLP vs. SJC)
- **Date of Birth (DOB):** Can it consider DOB as part of the matching process?

2. Handling Global Name Ethnicity Specific Phenomena

- **Arabic Names:** Can the system handle different segmentations of Arabic names in English? (e.g., Abd al-Rahman vs. Abdul Rahman vs. Abdarrahman)
- **Transliteration Standards:** Can it manage different transliteration standards, such as Pinyin and Wade-Giles for Chinese? (e.g., Xi Jinping vs. Hsi Chin-p'ing)
- **Spanish Last Names:** Can it handle Spanish last names with matronymics and patronymics? (e.g., Carlos Guzman Ramos vs. Carlos Guzman)

3. Fuzzy Matching of Required Entity Types

- **Entity Types:** Can the system handle fuzzy matching for a variety of entity types beyond personal names, such as:
  - Organization
  - Place
  - Address
  - Vehicle
  - Email Address

    - Phone number
    - Date
- **CIE Fields:** Ensure the system can handle the specific entity types associated with the reserved CIE fields used for the Master Person Index matching.

4. Fuzzy Matching of Records with Multiple Fields

- **Multiple Field Matching:** Can the system match records that include multiple fields, such as:
    - Name
    - Date of Birth
    - Place of Birth
    - Nationality
    - Spouse
    - Address
- **Intelligent Matching:** Does the system intelligently consider the matching results of all relevant fields to improve accuracy?

5. Providing a Matching Score

- **Threshold Flexibility:** Can the system provide a matching score to set cut-off thresholds for matches?
- **Accuracy Levels:** Can you adjust the matching score to be more stringent or lenient depending on the required accuracy for different use cases?

6. Accuracy of Fuzzy Name Matching

- **Low False Positives and Negatives:** Does the system minimize false positives and false negatives?
- **Assessment Capability:** Can you assess false negatives, ideally with an answer key for each name variant in the database?

7. Speed and Scalability

- **Real-Time Matching:** Can the system handle real-time matching requirements, such as those needed for security checks against a watch list?
- **Batch Processing:** Can it also efficiently handle batch processing for applications like marketing database updates?
- **Scalability:** Can the system scale to handle peak loads and large datasets?

8. Customizability

- **Specific Customizations:** Can the system be customized to handle:
    - Unconventional name aliases, nicknames, or abbreviations?
    - Specific field values to be ignored for matching purposes?
    - Adjusting the weights of fields to alter matching behaviors?

Evaluating fuzzy matching systems based on these criteria ensures that the chosen solution can effectively handle the diverse and complex matching requirements of the CIE. By addressing these detailed requirements, the CIE can maintain high data integrity and facilitate accurate and efficient data integration across all participating organizations.

Data Flow, Interoperability, and Solution Architecture

Implementation of the CIE Platform will require data to be shared smoothly between systems and people involved in the care of Fresno County residents. The data flow depicted in figure 2 is a high-level example of where data entry, data integration, or system to system data exchange will occur within the CIE Home Visitation pilot

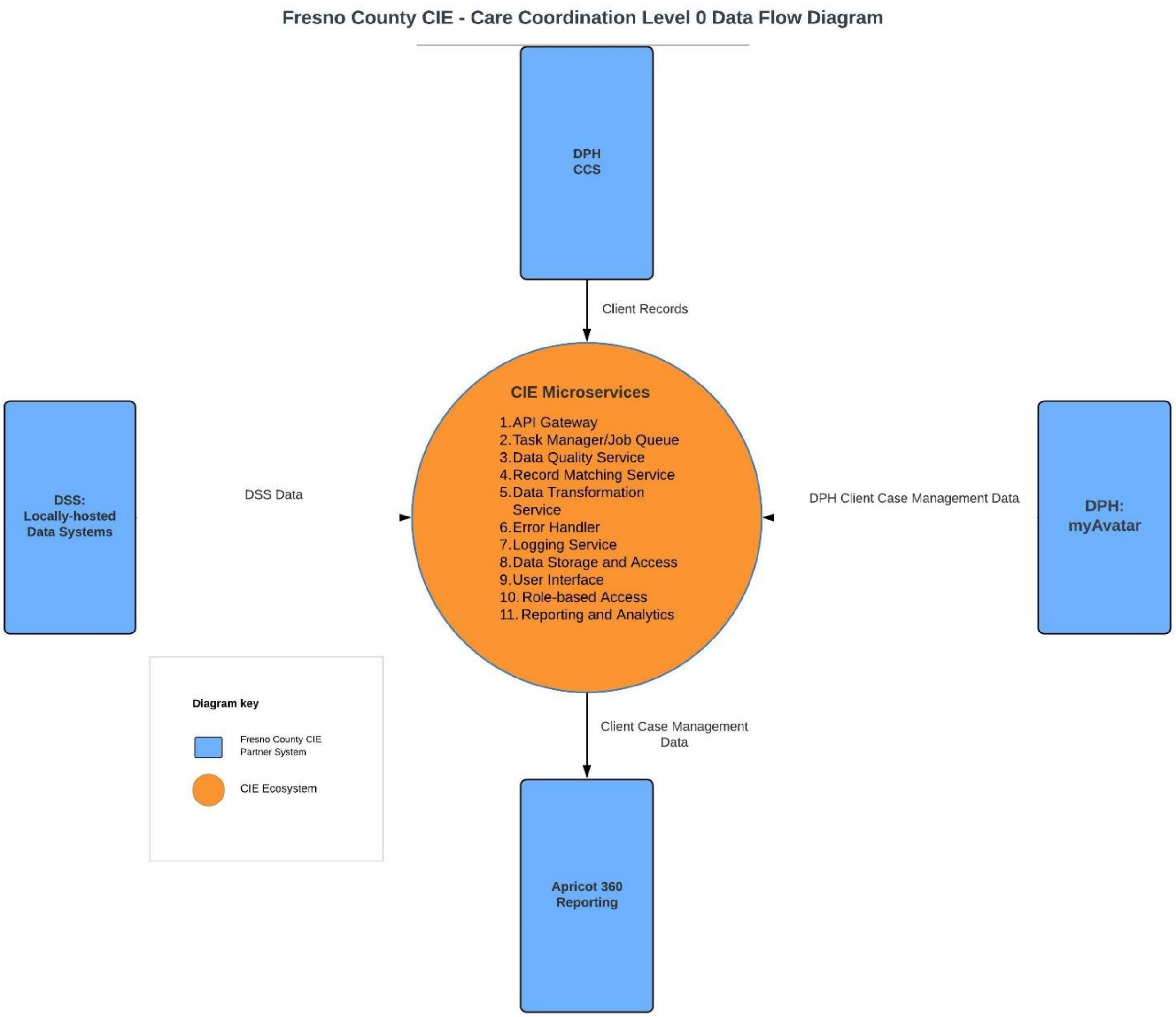

Fresno County CIE - Care Coordination Level 0 Data Flow Diagram
DPH CCS
Client Records
CIE Microservices
1. API Gateway
2. Task Manager/Job Queue
3. Data Quality Service
4. Record Matching Service
5. Data Transformation Service
6. Error Handler
7. Logging Service
8. Data Storage and Access
9. User Interface
10. Role-based Access
11. Reporting and Analytics
DSS: Locally-hosted Data Systems
DSS Data
DPH Client Case Management Data
DPH: myAvatar
Client Case Management Data
Apricot 360 Reporting
Diagram key
Fresno County CIE Partner System
CIE Ecosystem

Figure 2: Home Visitation Care Coordination Data Flow Diagram (Level 0)

Under this framework, systems of origin contributing to the CIE will send data through microservices such as API's, flat files or other secure data exchange protocols that meet established standards. Each system of origin would manage their own data submission in partnership with the CIE technical backbone vendor.

Overview CIE Microservices Processes and Data Flows

The proposed approach to the Fresno County Community Information Exchange (CIE) leverages a sophisticated microservices framework to ensure robust, scalable, and flexible data integration, centralization, and service delivery. This microservices architecture allows the CIE to efficiently manage and process the diverse data streams from various systems of origin, providing a seamless and dynamic platform for information exchange. By adopting a microservices framework, the CIE enhances its ability to respond to the evolving needs of the community, ensuring that critical services are delivered promptly and effectively while maintaining the highest standards of security and data integrity.

CIE Technical Components

Systems of Origin

Systems of origin of refers to the existing data systems of participating organizations that will send data to the CIE centralized data exchange. This integration ensures that crucial information from health, social services, education, and other sectors can be securely centralized and utilized within the CIE framework.

Systems of Origin Technical Considerations

Data Fields and Triggers

To ensure effective integration and timely data sharing within the Fresno County Community Information Exchange (CIE), a process targeting specific data fields from systems of origin must be developed. These targets will facilitate the process of capturing and transmitting relevant data changes to the CIE, facilitating regular updates and accurate data flow.

Key Components

- **Data Creation:** These data represent new record creation in the system of origin. They capture essential data fields relevant to the CIE and ensure the new information is shared in a timely way with the CIE.
- **Data Updates:** These data are submitted to the CIE when an existing record is changed in the system of origin. They monitor changes to specific data fields that are part of the common CIE dataset and ensure that these updates are promptly communicated to the CIE.
- **Dat Linkages:** The CIE will connect records within and between organizational data sets to support the basic functionality of data exchange between participating entities.

Data Fields to Monitor

- **Personal Identifiers:** Fields such as individual name, date of birth, and unique identification numbers (e.g., social security number, student ID) that are crucial for accurately matching records across systems.
- **Contact Information:** Updates to addresses, phone numbers, and email addresses to ensure that communication remains effective and up-to-date.
- **Service Eligibility and Enrollment:** Changes in eligibility status or enrollment in services such as healthcare programs, social services, and educational support.
- **Health and Behavioral Information:** Relevant health data, including diagnoses, treatment plans, and mental health status, which are critical for coordinated care and intervention.
- **Case Management Details:** Updates related to case notes, service plans, and follow-up actions that are essential for comprehensive case management.

Benefits

Implementing data field triggers within the systems of origin provides several key benefits:

- **Real-Time or Scheduled Data Sharing:** Ensures that any changes in the data are promptly reflected in the CIE, enabling real-time information access and decision-making.
- **Accuracy and Consistency:** Maintains the accuracy and consistency of data across all integrated systems, reducing the risk of discrepancies and errors.
- **Enhanced Coordination:** Facilitates better coordination among various service providers by ensuring that all parties have access to the most current and relevant information.
- **Automation and Efficiency:** Automates the data capture and sharing process, reducing the need for manual data entry and minimizing the potential for human error.

Origin System API Development

To facilitate seamless data integration within the Fresno County Community Information Exchange (CIE), there is a potential need to develop Application Programming Interfaces (APIs) for systems of origin that currently lack this capability. APIs are needed to enable automated, secure, and efficient data communication between diverse systems, though development of a workflow focused on the extraction of data from systems of origin onto a flat file or other portable form is another viable method for data exchange.

Key Aspects of API Development

- **Seamless Data Integration:** APIs enable the automated exchange of data between systems, ensuring that information flows smoothly and accurately into the CIE without the need for manual intervention.
- **Real-Time Data Sharing:** With APIs, data from the systems of origin can be shared in real-time, providing up-to-date information to all CIE participants and enhancing decision-making processes.
- **Standardization:** APIs help standardize data formats and protocols, ensuring compatibility and interoperability across various systems and platforms involved in the CIE.
- **Scalability:** Developing APIs allows the CIE to scale more effectively by facilitating the integration of additional systems and data sources as the network of participating organizations expands.
- **Efficiency and Automation:** APIs reduce the need for manual data entry and processing, increasing operational efficiency and minimizing the risk of human error.

Benefits of API Integration

- **Enhanced Coordination:** Facilitates better coordination among healthcare providers, social services, educational institutions, and other stakeholders by ensuring they have access to accurate and timely data.
- **Improved Data Quality:** Ensures that data shared with the CIE is consistent, reliable, and free from discrepancies, thereby improving overall data quality.
- **Streamlined Operations:** Automates routine data exchange processes, freeing up resources and allowing staff to focus on more critical tasks and interventions.
- **Security and Compliance:** APIs can be designed with robust security features to protect sensitive information, ensuring compliance with data privacy regulations and standards.

Implementation Considerations

- **Assessment:** Conduct a thorough assessment of the current systems of origin to identify those that lack API capabilities and require development.
- **Development:** Engage with IT professionals and API developers to design and build the necessary APIs, ensuring they meet the specific needs of the CIE.
- **Testing and Validation:** Implement rigorous testing and validation procedures to ensure the APIs function correctly and securely before full-scale deployment.
- **Training and Support:** Provide training and support to staff and partners to ensure they

understand how to use the new APIs effectively.

CIE API Gateway

The API Gateway component services as a centralized entry point for managing and directing API requests between external client systems of origin and the various microservices within the CIE framework.

Key Features

- **Request Routing:** The API Gateway efficiently routes incoming API requests to the appropriate microservices, ensuring that data is accurately and promptly delivered to the right destinations.
- **Security:** Implements advanced security measures, including authentication and authorization protocols, to protect sensitive data and ensure that only authorized users can access the system.
- **Rate Limiting and Throttling:** Manages and controls the flow of incoming requests to prevent system overloads and ensure optimal performance and reliability.
- **Data Transformation:** Handles data transformation and formatting, ensuring compatibility between different systems and facilitating seamless data exchange.
- **Monitoring and Logging:** Provides comprehensive monitoring and logging capabilities, enabling real-time tracking of API requests and system performance, and assisting in troubleshooting and system optimization.

Benefits

The API Gateway component enhances the efficiency, security, and scalability of the CIE microservices architecture. By centralizing the management of API requests, it simplifies the integration of diverse data systems and ensures consistent and reliable communication between all components. This facilitates a more cohesive and responsive CIE, capable of delivering timely and effective services to meet the needs of Fresno County residents.

Task Manager/Job Queue

The Task Manager/Job Queue orchestrates the scheduling, execution, and management of various tasks and background jobs within the system.

Key Features

- **Task Scheduling:** Allows for the scheduling of tasks at specific times or intervals, ensuring that routine processes such as data updates and synchronization are executed timely.
- **Job Queue Management:** Manages a queue of background jobs, prioritizing and distributing them across available resources to ensure efficient processing.
- **Scalability:** Provides the ability to scale task execution dynamically based on system load and demand, ensuring consistent performance even during peak times.
- **Monitoring and Alerts:** Includes monitoring capabilities to track task status and performance, with alerts for any failures or issues requiring attention.

Benefits

By managing and optimizing the execution of tasks, the Task Manager/Job Queue ensures that the CIE operates smoothly and efficiently, handling large volumes of data and complex workflows with reliability and precision.

Data Quality Service

The Data Quality Service ensures the accuracy, consistency, and reliability of the data within the CIE. It performs various checks and validations to maintain high data quality standards.

Key Features

- **Data Validation:** Validates incoming data against predefined rules and criteria to ensure accuracy and completeness.
- **Data Cleaning:** Identifies and corrects errors, inconsistencies, and duplicates in the data, improving its overall quality.
- **Monitoring:** Continuously monitors data quality and provides reports and alerts on any issues detected.
- **Standardization:** Ensures that data conforms to standard formats and protocols, facilitating seamless integration and interoperability.

Benefits

The Data Quality Service enhances the integrity and reliability of the data within the CIE, ensuring that all stakeholders can trust the information they receive and use it effectively for decision-making and service delivery.

Record Matching Service

The Record Matching Service identifies and links records belonging to the same entity across different data sources. This service ensures that the CIE can provide a comprehensive and unified view of individual records.

Key Features

- **Entity Resolution:** Uses sophisticated algorithms to match records that refer to the same entity, such as a person or organization, across multiple datasets.
- **Duplicate Detection:** Identifies and merges duplicate records to avoid redundancy and ensure data accuracy.
- **Confidence Scoring:** Assigns confidence scores to matched records to indicate the likelihood of a correct match, allowing for manual review if needed.

Benefits

By accurately linking related records, the Record Matching Service provides a holistic view of data, enhancing the CIE’s ability to deliver coordinated and comprehensive services.

Master Person Index (MPI)

The Master Person Index (MPI) is a fundamental component of the Fresno County Community Information Exchange (CIE) microservices architecture. It serves as a centralized database that uniquely identifies and maintains comprehensive records of individuals across various systems and data sources. The MPI ensures that each individual has a unique identifier, facilitating accurate data integration, matching, and retrieval.

Key Features

- **Unique Identifier Assignment:** Assigns a unique identifier to each individual, ensuring consistent and accurate identification across different systems and data sources.
- **Data Integration:** Consolidates data from multiple sources, including healthcare, social services, education, and other sectors, to create a single, unified record for each individual.
- **Record Matching and Linking:** Utilizes advanced algorithms to match and link records that pertain to

the same individual, even if the data is from disparate sources or contains variations in personal information.

- **Data Quality Management:** Maintains high data quality standards by identifying and resolving duplicate records, inaccuracies, and inconsistencies within the index.
- **Scalability:** Designed to handle large volumes of data and a growing number of records, ensuring it can scale with the expanding needs of the CIE.

Benefits

The Master Person Index offers several key benefits to the Fresno County CIE:

- **Enhanced Data Accuracy:** By providing a single, authoritative source of truth for individual identities, the MPI improves the accuracy and reliability of data used for service delivery and decision-making.
- **Improved Service Coordination:** Facilitates better coordination of services across different sectors by ensuring that all partners have access to the same comprehensive and accurate individual records.
- **Efficient Data Retrieval:** Simplifies data retrieval processes by allowing partners to access a unified record for each individual, reducing the time and effort required to gather and verify information.
- **Privacy and Security:** Enhances data privacy and security by ensuring that sensitive information is consistently managed and protected across the CIE.

Data Transformation Service

The Data Transformation Service converts data from its original format into a standardized format compatible with the CIE. This service ensures that data from diverse sources can be integrated and used effectively.

Key Features

- **Format Conversion:** Transforms data into the required format, ensuring compatibility with other systems and services within the CIE.
- **Data Mapping:** Maps data fields from the source format to the destination format, preserving data integrity and meaning.
- **Normalization:** Standardizes data values and structures to ensure consistency and facilitate seamless integration.

Benefits

The Data Transformation Service ensures that data from various sources can be efficiently integrated into the CIE, supporting interoperability and enhancing the overall functionality of the system.

Error Handler

The Error Handler is responsible for detecting, managing, and resolving errors within the CIE microservices architecture. It ensures that the system can handle issues gracefully and maintain operational integrity.

Key Features

- **Error Detection:** Identifies errors in real-time, including data processing errors, system failures, and integration issues.
- **Logging and Alerts:** Logs error details and sends alerts to administrators, enabling prompt response and troubleshooting.
- **Automated Recovery:** Implements automated recovery procedures for certain types of errors, minimizing downtime and service disruption.
- **Detailed Reporting:** Provides detailed error reports to assist in diagnosing and resolving issues.

Benefits

The Error Handler enhances the resilience and reliability of the CIE, ensuring that the system can quickly recover from issues and maintain continuous operation.

Logging Service

The Logging Service tracks and records system activities and events within the CIE microservices architecture. This service provides valuable insights for monitoring, troubleshooting, and auditing purposes.

Key Features

- **Activity Logging:** Records detailed logs of all system activities and events, including data transactions, user actions, and system operations.
- **Centralized Log Management:** Consolidates logs from various microservices into a centralized repository for easy access and analysis.
- **Real-Time Monitoring:** Enables real-time monitoring of system performance and activities, with capabilities to detect anomalies and issues.
- **Audit Trails:** Maintains comprehensive audit trails to support compliance, security, and forensic investigations.

Benefits

The Logging Service ensures comprehensive visibility into the operations of the CIE, supporting effective monitoring, troubleshooting, and compliance with regulatory requirements.

Data Storage and Access

Data Storage and Access is essential to ensure that all data within the Community Information Exchange (CIE) is secured at rest and readily accessible to authorized users based on agreed parameters within a Service Level Agreement or similar documentation. This component includes robust data management strategies to support high availability, security, and efficient access across multiple user groups.

Key Features

- **Data Centralization**: All data is stored in a centralized repository that supports real-time and on-demand data access for all integrated systems.

- **Data Archiving**: Archival solutions manage historical data efficiently, ensuring that older records are stored in a way that remains accessible for long-term analysis and compliance purposes.

- **Backup and Recovery**: Redundant storage and regular backups protect data integrity and support disaster recovery.

Benefits

- **High Availability**: Ensures data is accessible whenever needed by authorized users, supporting efficient data-driven decision-making.

- **Enhanced Security**: Centralized storage supports enhanced security protocols, including encryption and access controls, ensuring data is consistently protected.

- **Scalability**: Enables the system to handle expanding volumes of data as more organizations join the CIE.

User Interface (UI)

The User Interface (UI) enables authorized users to view integrated data from multiple sources through a streamlined, easy to access, and user-friendly portal. This centralized access point provides a comprehensive view of client information, presented based on the role of the user, promoting coordinated care and informed decision-making across sectors.

Key Components

- **Linked Record Access**: Allows authorized users to access a unified view of client records linked across various systems, including health, social services, and education.
- **Search and Filter Functionality**: Robust search and filter tools allow users to quickly locate specific client records and view relevant data based on parameters such as service type, date, or organization.
- **Data Visualization**: Visual dashboards and summaries present complex data in an accessible format, allowing users to easily interpret information across multiple domains.

Benefits

- **Enhanced Coordination**: Provides a single access point to view comprehensive client information, improving collaboration among service providers.
- **Improved Decision-Making**: Access to integrated client data enables providers to make well-informed decisions and deliver tailored services.
- **Time Efficiency**: The UI design reduces time spent navigating disparate systems, allowing users to focus on service delivery.

Role-Based Access to the Centralized System

Role-Based Access to the Centralized System ensures data security by controlling user access to sensitive information based on their role within the CIE. This role-based approach supports data privacy, compliance, and ensures that users only access data pertinent to their responsibilities.

Key Components

- **Role Definitions and Permissions**: Permissions are assigned based on predefined roles, ensuring users only access data and functions necessary for their tasks.
- **Access Control Policies**: Enforces strict access control policies that align with privacy regulations, limiting exposure of sensitive information to unauthorized users.
- **Audit Trails**: Comprehensive logging of user access and actions to maintain accountability and support data governance practices.

Benefits

- **Data Security**: Role-based access minimizes exposure of sensitive data, protecting client privacy.
- **Regulatory Compliance**: Adheres to data privacy laws and regulations by enforcing role-specific access restrictions.
- **Customizable Access**: Flexible role definitions accommodate various user roles, enabling tailored access

based on organizational needs.

Reporting and Analytics

Reporting and Analytics capabilities enable data-driven insights by providing standardized report and additional tools to access, analyze, and visualize data within the CIE. These tools help users monitor performance, track trends, and make informed decisions to improve service delivery.

Key Components

- **Data Visualization**: Intuitive visual dashboards present data insights, allowing users to interpret complex data easily and make informed decisions.
- **Automated Reporting**: Scheduled reports provide regular updates on key metrics, helping organizations track progress and identify areas for improvement.
- **Predictive Analytics**: Advanced analytics enable forecasting and trend analysis, assisting in proactive decision-making and resource allocation.

Benefits

- **Enhanced Decision-Making**: Analytics provide actionable insights, helping organizations tailor services and respond to emerging trends.
- **Resource Optimization**: Data-driven insights allow for better resource allocation and prioritization of services.
- **Transparency and Accountability**: Regular reporting fosters transparency, supports accountability, and aids in meeting compliance and performance standards.

Technical View of Dataflows and Technology Considerations

This section offers an in-depth view of the potential microservices which could facilitate the integration, management, and exchange of data within the Fresno County CIE, along with proposed technologies currently in the market which have capabilities to support the described functionality. By detailing the workflows for data capture, processing, and dissemination, this section ensures that all stakeholders understand the critical pathways and technologies that support efficient and secure information sharing. These workflows are designed to enhance interoperability, maintain data integrity, and ensure timely access to accurate information, ultimately driving better outcomes for the community.

Operational Data Flows at the System of Origin

System of Origin End Users will trigger the transaction of data to the CIE core system through the following actions:

1. **Creating a New Record:** Adding a new entry that is relevant to the CIE dataset.
2. **Updating an Existing Record:** Modifying an existing entry within the fields that are part of the common CIE dataset.

Upon execution of either of these triggering events, the internal system will initiate an HTTPS call to the CIE API endpoint. This call will include:

1. **Authentication Information:** API key specific to the organization.
2. **Record Data (in JSON format):**
    - **Organization-Specific Unique Identifier:** The unique identifier for the record within the organization.

- **Complete Record (for new entries):** Sent via HTTPS POST, this record will contain:
    1. **Reserved Fields:** Data fields with definitions agreed upon by all CIE participants.
    2. **Custom Fields:** Data unique to the submitting organization.
- **Partial Record (for updates):** Sent via HTTPS PATCH, containing only the fields that have been updated.
- **User Identifier:** The specific User_ID of the end user who created or updated the record within the organization.
- **Timestamp:** The exact time of the transaction, recorded in UNIX milliseconds.

This approach ensures that data is consistently and securely transmitted to the CIE core system, maintaining data integrity and enabling effective interoperability among all participating entities.

CIE API Endpoint

When the CIE API endpoint receives an API call, it will undertake the following actions:

1. **Logging Information:** Send logging information to the Logging Service (LogS) at each stage of the API endpoint process.
2. **Basic Checks for Required Fields and Values:**
    - If checks pass, continue processing.
    - If checks fail, route to the Exception Handler Service (EHS).
3. **Authenticate API Key:** Verify the API key to ensure the call is from an authorized source.
4. **Technical Format Validation:** Perform a basic check to ensure the correct technical formatting (HTTPS, POST, PATCH, or GET).
5. **Data Parsing:** Parse the incoming data fields.
6. **Data Validation on Reserved Fields:** Validate the data against a pre-defined system mapping for:
    - Content format (e.g., INT, varchar, JSON, timestamp, BLOB, BIT, etc.).
    - Content length.
    - Presence of required fields.
    - Properly formed JSON payload.
7. **Insert Organization-Specific Identifiers:**
    - Insert an Org_ID specific to the service provider of origin.
    - Insert an Action value indicating the operation (Insert, Update).
8. **Transaction Management:**
    - Insert a unique Transaction_ID into the payload for logging purposes.
9. **Payload Routing:**
    - If there are no errors and the HTTP method is POST or PATCH, pass the payload to the Task Master Job Queue (TMJQ), which then sends it to the Record Matching Service (RMS).
    - If errors are detected, route the payload to the Exception Handler Service (EHS).

This process ensures secure, accurate, and efficient handling of data transactions within the CIE, maintaining data integrity and providing robust error management.

Examples of Applicable API Gateways

To facilitate secure, efficient, and scalable data integration within the Fresno County Community Information Exchange (CIE), a robust API Gateway is essential. The following are examples of applicable API Gateways that can be considered for implementation:

1. WSO2 API Manager

- **Description:** WSO2 API Manager is an open-source API management solution that provides full lifecycle API management, including API creation, publishing, lifecycle management, application

development, access control, rate limiting, analytics, and monitoring.
- **License:** Apache 2.0
- **Resource Link:** WSO2 API Manager

2. **Microsoft Azure API Management**
    - **Description:** Azure API Management is a fully managed service that enables enterprises to publish, secure, transform, maintain, and monitor APIs. It offers a platform for API management, ensuring high availability and scalability.
    - **Resource Link:** Microsoft Azure API Management
3. **Tyk API Gateway**
    - **Description:** Tyk is an open-source API Gateway and Management platform that provides API analytics, developer portals, and security capabilities such as rate limiting and quota management. It is available as both a commercial and open-source solution.
    - **Resource Link:** Tyk API Gateway
4. **Google API Gateway**
    - **Description:** Google API Gateway provides a fully managed gateway to deploy, secure, and monitor APIs at scale. It is built on the same infrastructure as Google Cloud, offering security, high availability, and low latency.
    - **Resource Link:** Google API Gateway
5. **KrakenD**
    - **Description:** KrakenD is an ultra-performant open-source API Gateway that provides high throughput, low latency, and scalability. It is designed to aggregate multiple microservices into a single endpoint and supports advanced security and transformation features.
    - **Resource Link:** KrakenD

Task Master Job Queue (TMJQ)

When the Task Master Job Queue (TMJQ) receives the payload, it follows these steps to ensure proper task management and data processing:

1. **Logging Information:** Sends log entries to the Logging Service (LogS) at each stage of the queue process.
2. **Basic Checks for Required Fields and Values:**
    - If checks pass, continue processing.
    - If checks fail, route to the Exception Handler Service (EHS).
3. **Task Ingestion:**
    - **Task Creation:** Create a new task by assigning it a unique Task_ID.
    - **Metadata Assignment:** Record the Origin_Org_Id (Org_ID value), Created_At timestamp (Unix milliseconds), Last_Modified timestamp (Unix milliseconds), Current_Stage, and Last_Stage.
    - **Task Payload Entry:** Create an entry in the Tasks_Payload table, including:
        - Task_ID (from above).
        - Unique Payload_ID.
        - Payload field containing the data.
4. **Microservices Coordination:** Acts as the central point of control, sending the task to the following microservices in order and processing their results:
    - **Data Quality Service (DQS):** Ensures data integrity and accuracy.
    - **Record Matching Service (RMS):** Matches and links records across datasets.
    - **Data Transformation Service (DTS):** Transforms data into required formats.
    - **API Service - Outbound (API):** Manages outbound communication with target systems.
        - **Target Systems Integration:** Supplies target URLs, authentication credentials, and other necessary information for external data reception. Preferred method is via API endpoint,

with an alternative option being an SFTP server.

5. **Scheduled Tasks Initiation:** Capable of initiating tasks on a scheduled basis to proactively fulfill CIE technical requirements, such as:
    - **CSV Data Exports Retrieval:** Sending tasks to retrieve CSV data exports from partner-controlled, external SFTP servers for CIE processing.
    - **Updated Records Checking:** Sending tasks to partner-built API endpoints to check for updated records via local connectors (ODBC, direct SQL connection, etc.) and generate CIE-formatted payloads for processing.
6. **Integration with Existing Systems:** Acts as an overlay for an existing task/job management queue system or directly implements an existing task/job queue management system. The steps outlined above are illustrative and may vary based on the specific system used.

This comprehensive process ensures efficient, accurate, and secure handling of tasks within the CIE, maintaining data integrity and supporting coordinated service delivery.

Examples of applicable job queue systems:

For the effective management of tasks and queues within the Fresno County Community Information Exchange (CIE), selecting a robust task and message queue system is essential. The following are examples of applicable systems that can be considered for implementation:

1. **BullMQ**
    - **Description:** BullMQ is a powerful, fast, and feature-rich job queue for Node.js applications. It is designed to handle jobs and manage task scheduling, retries, and concurrency.
    - **License:** GPL
    - **Resource Link:** BullMQ
2. **Amazon Simple Queue Service (SQS)**
    - **Description:** Amazon SQS is a fully managed message queuing service that enables the decoupling and scaling of microservices, distributed systems, and serverless applications. It offers reliable, highly-scalable, and secure message queuing.
    - **Resource Link:** Amazon Simple Queue Service
3. **Celery**
    - **Description:** Celery is an asynchronous task queue/job queue based on distributed message passing. It is focused on real-time operation but supports scheduling as well. Celery is used in production systems to process millions of tasks per day.
    - **License:** BSD
    - **Resource Link:** Celery
4. **RabbitMQ**
    - **Description:** RabbitMQ is a widely-used open-source message broker that implements the Advanced Message Queuing Protocol (AMQP). It is known for its reliability, flexibility, and support for multiple messaging protocols.
    - **License:** Apache License
    - **Resource Link:** RabbitMQ
5. **Apache Kafka**
    - **Description:** Apache Kafka is a distributed event streaming platform capable of handling trillions of events a day. It is designed for high throughput, low latency, and fault-tolerant data streaming and processing.
    - **Resource Link:** Apache Kafka

Selecting the right task and message queue system is crucial for ensuring the efficient operation of the CIE. The systems listed above offer a variety of features and capabilities that can meet the needs of different components within the CIE, including task scheduling, message passing, and real-time data processing. Each option provides unique advantages, and the final choice should be based on specific project requirements, scalability needs, and integration capabilities.

Data Quality Service (DQS)

When the Data Quality Service (DQS) receives the payload, it follows these steps to ensure the data meets quality standards:

1. **Logging Information:** Sends log entries to the Logging Service (LogS) at each stage of the data quality checking process.
2. **Basic Checks for Required Fields and Values:**
   - If checks pass, continue processing.
   - If checks fail, route to the Exception Handler Service (EHS) for non-transient error handling.
3. **Data Cleaning Process:**
   - **Typo Correction:** Identifies and corrects common typographical errors.
   - **Standardization:** Ensures consistent capitalization and formatting of entries.
   - **Invalid Entries Removal:** Eliminates entries deemed not allowed within a multiple organization dataset, such as “N/A” and “Not Applicable”.

This structured process ensures that the data is accurate, standardized, and ready for further processing within the CIE, enhancing the reliability and usability of the information shared across participating organizations.

Examples of existing applicable systems:

For the effective transformation and cleansing of data within the Fresno County Community Information Exchange (CIE), selecting a data transformation system is essential. The following are examples of applicable systems that can be considered for implementation:

1. Osmos

- **Description:** Osmos provides a comprehensive data transformation and integration platform that simplifies the process of cleaning, transforming, and importing data from various sources. It offers a user-friendly interface and powerful tools to automate data workflows, ensuring data is accurate and ready for analysis.
- **Resource Link:** Osmos

2. First Logic

- **Description:** First Logic offers advanced data cleansing solutions designed to ensure the accuracy and integrity of data. Their platform provides tools for data quality improvement, including standardization, validation, and enrichment, helping organizations maintain high-quality data for critical operations.
- **Resource Link:** First Logic

3. Databricks

- **Description:** Databricks is a unified data analytics platform that provides tools for data engineering, machine learning, and collaborative analytics. It enables organizations to process large volumes of data efficiently, perform complex transformations, and integrate data from various sources, facilitating robust data workflows and analytics.
- **Resource Link:** Databricks

Selecting the right data transformation system is crucial for ensuring the accuracy, quality, and usability of data within the CIE. The systems listed above offer a variety of features and capabilities that can meet the diverse needs of the CIE, including data cleansing, transformation, and integration. Each option provides unique advantages, and the final choice should be based on specific project requirements, data volume, and integration capabilities.

Record Matching Service (RMS)

When the Record Matching Service (RMS) receives a client payload from the Task Manager, it performs the following steps to ensure accurate record matching and data integration:

1. **Logging Information:** Sends log entries to the Logging Service (LogS) at each stage of the record matching process.
2. **Basic Checks for Required Fields and Values:**
   - If checks pass, continue processing.
   - If checks fail, route to the Exception Handler Service (EHS) for non-transient error handling.
3. **Data Parsing:**
   - Parses the data fields specifically used for record matching.
4. **System Fields Check:**
   - Ensures the presence of required system fields: Org_ID, Transaction_ID, Client_ID, Action.
5. **Master Person Index (MPI) Search:**
   - Searches the MPI for a pre-existing instance of the Client_ID.
   - If found:
     - Appends the MPI_ID field value and the Org_Client_ID field value (a JSON object with key pairs of "Org_ID":"Client_ID" specific to each organization) to the current transaction payload.
   - If not found:
     - Calls the Fuzzy Matching Service (FMS), which:
       - Indexes fields with possible Personal Identifying Information (PII).
       - Initiates a search within the MPI for records with matching PII data.
6. **Fuzzy Matching Process:**
   - **Single Match Found:**
     - If the FMS finds a single MPI record with 100% match fidelity:
       - Updates the Org_Client_ID field (JSON) by appending the Org_ID as a new entry in the JSON object.
       - Updates the Last_Modified date with a Unix milliseconds timestamp.
       - Appends the MPI_ID and Org_Client_ID field to the current transaction payload.
   - **Multiple Matches Found:**
     - If the FMS finds multiple records with a high match score:
       - Places the highest scoring records into a manual review queue.
       - Alerts a CIE data specialist or the submitting user at the system of origin based on the Org_ID/User_ID fields contained within the payload.
       - Awaits manual input by an end user on the action to take. The manual review queue is managed within the FMS.
   - **No Matches Found:**
     - If no records meet the match threshold:
       - Creates a new MPI record, including:
         - An automatically generated, unique MPI_ID.
         - The Org_Client_ID field (JSON) with the Org_ID key pair as a sole entry.
         - A Created_By field (JSON) to track the originating organization and user.
         - Created_On and Last_Modified dates with Unix milliseconds timestamps.
       - Appends the MPI_ID and Org_Client_ID field to the current transaction payload.
7. **Completion:** Once the RMS has processed the data, the new data payload, including the necessary

identifiers and updates, is returned to the Task Manager for further handling.

Resources for Evaluation:

Selecting an effective fuzzy matching system is critical for ensuring accurate record matching and data integration within the Fresno County Community Information Exchange (CIE). The following resources provide comprehensive guidance and options for evaluating and choosing the right fuzzy matching solution.

Evaluation Guides

- **Fuzzy Matching System Evaluation Requirements:** This guide provides a detailed list of questions and criteria to consider when evaluating fuzzy matching vendors. It helps organizations identify the most suitable solution based on specific needs, capabilities, and performance requirements.

Open Source Projects

- **GitHub: Data Matching Software:** A repository of open source data matching projects available on GitHub. These projects offer various tools and libraries for implementing fuzzy matching algorithms and can be a valuable resource for developing custom solutions.

Commercial Vendors for Consideration

1. **WinPure**
   - **Description:** WinPure Clean & Match API is a comprehensive data matching and cleansing solution that provides advanced fuzzy matching capabilities. It is designed to handle large datasets and deliver accurate, reliable results for data integration and record matching.
   - **Resource Link:** WinPure Clean & Match API
2. **First Logic**
   - **Description:** First Logic Match IQ is an advanced data matching solution that offers powerful fuzzy matching algorithms. It helps organizations accurately match and deduplicate records, improving data quality and consistency.
   - **Resource Link:** First Logic Match IQ
3. **Senzing**
   - **Description:** Senzing provides real-time entity resolution and fuzzy matching capabilities, ensuring accurate and efficient data matching across various datasets. Its scalable platform is designed to handle complex data matching scenarios, enhancing data quality and integration.
   - **Resource Link:** Senzing
4. **Databricks**
   - **Description:** Databricks Product Matching with ML offers machine learning-based fuzzy matching solutions. It provides tools for advanced data matching, integration, and analysis, leveraging the power of the Databricks platform to deliver high performance and accuracy.
   - **Resource Link:** Databricks Product Matching with ML

Evaluating and selecting the right fuzzy matching system is crucial for the successful implementation of the CIE. The resources and vendors listed above provide a range of options, from open source projects to advanced commercial solutions, ensuring that the CIE can find a suitable match for its specific data matching needs. Each option offers unique features and benefits, and the final choice should be based on thorough evaluation and alignment with the CIE's operational requirements.

Data Transformation Service (DTS)

When the Data Transformation Service (DTS) receives the payload, it follows these steps to ensure the data is correctly transformed and mapped to the appropriate organizational formats:

1. **Logging Information:** Sends log entries to the Logging Service (LogS) at each stage of the data transformation process.

2. **Basic Checks for Required Fields and Values:**
    - If checks pass, continue processing.
    - If checks fail, route to the Exception Handler Service (EHS) for non-transient error handling.
3. **Data Transformation Process:**
    - **Reading Org_ID Values:** Reads each Org_ID value from the payload.
    - **Checking Data Access Rules:** Verifies the data access rules for each Org_ID, which govern which organizations accept what data from which other organizations. This ensures that data is only shared according to established agreements and preferences.
        - **Example Scenarios:**
            - **Organization A as Source:** Organization A may act as the definitive source of specific data for other organizations but does not ingest data in return. Therefore, when Organization A pushes a record into the CIE, it is sent to all other organizations. However, when other organizations push data, the DTS disallows any payload creation for Organization A.
            - **Updating Access Rules:** If Organization A decides to consume data from Organization C (a definitive source of a different dataset), the data access rules can be updated to include Organization A in the DTS payload generation when data comes from Organization C.
    - **Finding Data Maps:** Locates the appropriate data map for each Org_ID that is accepting the payload from the system of origin. This map provides a blueprint for the fields that the organization will accept, their equivalent field names in the organization's data structure, and any additional relevant information.
        - **Field Acceptance:** Some organizations may restrict overwriting certain fields (e.g., name, address, DOB) to protect immutable or sensitive information.
    - **Building New Payloads:** Constructs a new record payload for each organization based on the data from the system of origin and the data mapping document. Fields without data are excluded from the payload to ensure that default values or existing data handling procedures are respected.
        - **New vs. Existing Records:** For new client records, the payload includes all relevant fields. For existing records, the action taken is a PATCH() to update only changed fields, rather than a PUT() which would replace the entire target record.
4. **Returning DTS Payload:**
    - **To TMJQ:** Returns the transformed DTS payload to the Task Master Job Queue (TMJQ).
    - **MPI Update:** If this is a new client record, upon receiving the DTS payload, the TMJQ sends an update to the Master Person Index (MPI) within the Record Matching Service (RMS) to reflect which organizations have the client within their systems and the corresponding matching fields based on the DTS-generated payload.

Technical Notes on Data Transformation

- **Common Technology:** Data transformation systems are widely used within data pipelines. The CIE can leverage existing solutions or commercial vendors for this service.
- **Solutions for Evaluation:**
    - **Osmos:** Osmos Data Transformation
    - **Apache NiFi:** Apache NiFi
    - **Databricks:** Databricks
    - **Rapidfuzz (MIT License):** Rapidfuzz

By following this detailed process, the DTS ensures that data is accurately transformed and mapped, facilitating efficient and secure data sharing within the CIE while respecting the unique requirements and preferences of each participating organization.

Logging Service (LogS)

The centralized Logging Service (LogS) is an essential component of the CIE system, tasked with tracking various metrics and events across the infrastructure. It ensures comprehensive monitoring and logging to maintain system health, performance, and security. The LogS will perform the following functions:

Key Logging Areas

1. **Client Records Tracking:**
   - Logs new or updated client records as they progress through the CIE system to completion.
2. **Hardware and Operating System Metrics:**
   - Monitors health and performance metrics of hardware and operating systems.
3. **Network Health Metrics:**
   - Tracks network health and performance to ensure reliable connectivity.
4. **Service Health Metrics:**
   - Monitors the health and performance of critical services (API, TMJQ, DQS, FMS, and DTS).
5. **Security Monitoring:**
   - Tracks security-related events and potential threats to ensure system integrity and compliance.

Minimum Functional Requirements for Logging Services

The Logging Service must be capable of accepting logging information from a diverse array of sources through multiple interfaces. Additionally, it should include the following functionalities:

1. **Secure User Logins:**
   - Implement Two-Factor Authentication (2FA) or other advanced methods to secure user logins.
2. **User Roles and Access Levels:**
   - Provide fine-grained control over user roles and access levels to ensure appropriate permissions.
3. **External Alerting:**
   - Enable alerting through external channels (email, SMS, Slack, etc.) based on user-defined criteria, including but not limited to:
     - **CPU, RAM, and Drive Space Usage:** Alerts based on hardware resource utilization.
     - **Overall Transaction Latency:** Monitors the time it takes for an individual client record to traverse the CIE.
     - **Service Transaction Latency:** Tracks latency for individual services.
     - **CIE Error Rates:** Alerts on error rates per second, minute, hour, and percentage.
     - **Service Error Rates:** Monitors error rates for individual services.
     - **Traffic Fluctuations:** Alerts on significant increases or decreases in traffic into the CIE system.
4. **Live Visual Reporting Dashboards:**
   - Provide real-time dashboards displaying all metrics with additional filtering options, such as by participating organization.
5. **In-Depth Metric Analysis:**
   - Allow detailed inspection from any single reporting metric to specific time frames, individual transactions, hardware, or software components.
6. **Search-Based Filtering:**
   - Enable search-based filtering of logged data for easy retrieval and analysis.
7. **Reporting Exports:**
   - Support exporting reports for further analysis and record-keeping.
8. **Compliance:**

- Ensure compliance with relevant data standards such as HIPAA, FERPA, and other applicable regulations.

Examples of Centralized Logging Services

Centralized logging services are essential for monitoring, troubleshooting, and maintaining the health and performance of the Fresno County Community Information Exchange (CIE). These services provide comprehensive logging, real-time analytics, and alerting capabilities to ensure the system operates smoothly and securely. The following are examples of centralized logging services that can be considered for implementation:

1. **Elasticsearch**
   - **Description:** Elasticsearch is a powerful open-source search and analytics engine designed for scalability and high performance. It allows organizations to search, analyze, and visualize data in real-time, making it ideal for centralized logging and monitoring.
   - **Resource Link:** Elasticsearch
2. **New Relic**
   - **Description:** New Relic offers a comprehensive suite of tools for application performance monitoring and real-time analytics. It provides detailed insights into system performance, error tracking, and user interactions, enabling proactive maintenance and troubleshooting.
   - **Resource Link:** New Relic
3. **Splunk**
   - **Description:** Splunk is a robust platform for searching, monitoring, and analyzing machine-generated data. It offers powerful capabilities for log management, data visualization, and real-time analytics, helping organizations to quickly identify and resolve issues.
   - **Resource Link:** Splunk
4. **Signoz**
   - **Description:** Signoz is an open-source observability platform designed for monitoring and analyzing application performance and logs. It provides real-time metrics, traces, and logs, allowing organizations to gain deep insights into their system's behavior and performance.
   - **Resource Link:** Signoz

Choosing the right centralized logging service is critical for ensuring the effective monitoring and management of the CIE system. The services listed above offer a variety of features and capabilities that can meet the diverse needs of the CIE, including real-time analytics, error tracking, and data visualization. Each option provides unique advantages, and the final choice should be based on specific project requirements, scalability, and integration capabilities.

Error Handling Service (EHS)

The Error Handling Service (EHS) is a critical component in managing the complexities of a microservices architecture within the CIE. Given the inherent scalability, robustness, and performance benefits of microservices, there is an increased complexity in error handling. Errors can arise from typical system issues, such as programmatic bugs or data exceptions, as well as from factors like network latency, system/vendor outages, or hardware problems. These errors are classified into two types:

1. **Non-Transient Errors:** Persistent errors, such as software bugs, that continue to occur unless fixed. These errors require immediate attention and resolution.
2. **Transient Errors:** Temporary errors that occur for a short duration due to issues like network outages or high request loads. These errors are usually resolved by retrying the process.

Error Handling Methodologies

1. Non-Transient Errors

Non-transient errors are persistent and require logging and immediate resolution.

- **Logging:** Log non-transient errors in the central logging service (LogS).
- **No Retry:** Do not retry the process that triggered the error.
- **Severity-Based Alerts:**
    - **Severity Level Classifications:**
        - **Severity Level 1 (Critical Impact/System Down):** Complete microservice outage.
        - **Severity Level 2 (Significant Impact/Severe Downgrade):** Severe service degradation.
        - **Severity Level 3 (Minor Impact):** Most of the microservice is functioning properly.
        - **Severity Level 4 (Low Impact/Informational):** Informational issues with minimal impact.
    - **Alerts:** For Severity 1 and Severity 2 errors, send alerts via email, SMS, or instant messaging (e.g., Slack) to on-call engineers for immediate troubleshooting and resolution.

2. Transient Errors

Transient errors are temporary and often resolved through retry mechanisms.

- **Logging:** Log transient errors in the central logging service (LogS).
- **Retry Mechanism:**
    - **Initial Retry:** The process or transaction that triggered the transient error is requeued in the Task Master Job Queue (TMJQ) and resent to the specific microservice for processing.
    - **Second Retry:** If the process fails again, it is requeued with an additional delay to avoid overwhelming the microservice with retry attempts.
    - **Final Attempt:** After a third failure, the error is marked as permanent, and the system of origin is informed of the new status.
- **Alerting on Repeated Failures:** If a high number of transient failures occur for a specific microservice or within the CIE system, the central logging service should alert on-call engineers for troubleshooting.

The Error Handling Service (EHS) provides a structured approach to managing both persistent and temporary errors in a microservices architecture. By implementing comprehensive logging, severity-based alerts, and retry mechanisms, the EHS ensures the resilience and reliability of the CIE system, enabling prompt resolution of issues and maintaining system performance and availability.

Partner Technical Systems Review

myAvatar – Department of Public Health

myAvatar™ is a behavioral health EHR that offers a recovery-focused suite of solutions leveraging real-time analytics, AI, and clinical decision support to drive value-based care.

Technical Capabilities and Considerations

- **Data Standard:** myAvatar's data schema adheres to the Fast Healthcare Interoperability Resources (FHIR) standard, widely adopted across various agencies and systems, enhancing interoperability.
    - **Resource Link:** FHIR Overview
- **API Capabilities:**
    - Current on-premises installations lack inherent API capabilities. However, the Carefabric upgrade enables an array of API connections.
    - Without the upgrade, data access relies on third-party connections (e.g., ODBC) to extract, insert, and update data within the InterSystems Cache database. This method, previously used by the Department of Public Health, has been inactive for eight years.

Use Case within CIE

- **Data Integration:** myAvatar will consume data pushed from CalSAWS via the Department of Social Services' Data Systems.

Data Management

- **Database System:** InterSystems Cache (v2017.2), a high-performance system supporting dynamic data objects (XML, JSON) and SQL querying.
  - **Resource Link:** InterSystems Cache
- **Custom Fields:**
  - Can create, export, and import custom fields.

Data Access and Permissions

- Supports data permissions down to the row and field level.

Data Security

- Uses built-in authentication for its user interface. Authentication for third-party/custom solutions is either via operating system-level users or accounts within the myAvatar user base.

Integration Limitation

- Current on-premises installations lack inherent API capabilities. The Carefabric upgrade can enable API connections. Otherwise, data access relies on third-party connections (e.g., ODBC) to the InterSystems Cache database.

Department of Social Services Data Systems

DSS locally manages a suite of tools and applications designed to help organizations collect, analyze, and present business data, enabling users to gather, process, and visualize data from various sources.

Technical Capabilities and Considerations

- **Enterprise Level Application:** DSS data systems provide robust capabilities for data analysis and visualization.
- **API Capabilities:**
  - Can make calls to external services.
  - Can answer API calls from external services.

Use Cases

- **Data Integration:** DSS data systems have the capability to supply CalSAWS information to the CIE, serving as a centralized data store.

Data Management

- **Database System:** Locally hosted databases with highly adaptable and scalable systems supporting SQL querying.
- **Custom Fields:**
  - Can create, export, and import custom fields.

Data Access and Permissions

- Supports data permissions down to the row and field level, configurable per group and user.

Data Security

- The specifics of API authentication (LDAP, Fusion Middleware, etc.) depend on the Department of Social Services' security implementation.

Integration Limitation

- DSS Data Bases can serve as a potential intermediate data store for CalSAWS. Adding new data fields directly to CalSAWS requires regional and state approval, taking 8 months to 3 year, making changes to source data a lengthy process.

Apricot 360 – Fresno County Superintendent of Schools

Apricot 360 is an enterprise system designed for small to mid-sized nonprofit organizations. It offers an all-in-one platform allowing organizations to define their datasets, reporting, and dashboards to suit their missions.

Technical Capabilities and Considerations

- **API Capabilities:**
  - Cannot make or answer API calls directly; relies on third-party systems (Workato, Zapier).
  - **Resource Links:**
    - Apricot API Integration
    - Apricot SFTP Imports
- **Automated SFTP Imports/Exports:** Available as an add-on, based on customized reports scheduled within Apricot 360.
  - **Resource Link:** Scheduling Reports

Use Cases

- **Reporting:** Will be used for reporting, ingesting data from myAvatar but not from CalSAWS.

Data Management

- **Custom Fields:**
  - Can create, export, and import custom fields.

Data Access and Permissions

- Supports data permissions down to the row and field level, configurable per group and user.

Data Security

- Uses built-in authentication for user interface access. SFTP integration requires an RSA SSH key for import.

Integration Limitation

- Direct API calls are possible only through registered third-party vendors in Workato or Zapier, adding complexity and cost. Automated SFTP imports cannot provide real-time updates, causing delays in data integration.

CCS Community Health Record (CHR) System – Department of Public Health

The CCS CHR is a CIE developed with data interoperability as a key component, aiming to provide a comprehensive view of client information to maximize positive outcomes. Fresno Department of Public Health has 150 end users and 2000+ clients in the system with relatively low traffic levels.

Technical Capabilities and Considerations

- **Data Interoperability:** Data is pre-cleaned by CCS, with a focus on interoperability.
- **API Capabilities:**
    - Can initiate and receive API calls.
    - Can perform scheduled data transmissions to API endpoints.
    - Utilizes Redox middleware to adhere to HL7 standards.
    - Prefers responding to external data requests via API calls due to system intensity of data update triggers.
    - Can send payloads containing only updated fields.

Use Cases

- **Integration:** The Department of Public Health will use CCS to manage data and case management for multiple external CBOs, with identifying client information (non-PII) pulled into the Master Person Index (MPI) for basic reporting.

Data Management

- **Custom Fields:**
    - Can create, export, and import custom fields.

Data Access and Permissions

- Supports data permissions down to the row level, configurable by roles and users.

Data Security

- Uses OKTA SSO for individual user logins.
- API authentication is managed through API keys and SSL.

Integration Limitation

- No significant limitations identified.

These detailed system breakdowns highlight the technical capabilities, integration limitations, and specific use cases for each system within the CIE. This comprehensive understanding is essential for ensuring seamless data integration and management across all participating organizations.

Implementing a Legal Framework for the Community Information Exchange

This section outlines the legal framework and best practices for data sharing between community partners within a Community Information Exchange framework, focusing on compliance with key privacy laws such as HIPAA (Health Insurance Portability and Accountability Act) and FERPA (Family Educational Rights and Privacy Act). The section is structured to assist healthcare systems, public health entities, human services, school districts, and community-based organizations in California to support sharing data. It details the necessary legal instruments and compliance measures, the operational roles of agents, and the process steps for legal data sharing.

Developing a Master Data Sharing Agreement Framework

A Master Data Sharing Agreement (MDSA) is a comprehensive document that outlines the overarching framework for data sharing among all participating entities in a Community Information Exchange (CIE). This agreement ensures that all parties adhere to standardized protocols and legal requirements, fostering trust and collaboration. The MDSA serves as a foundational document that individual Data Use Agreements (DUAs), Data Sharing Agreements (DSAs), and Business Associate Agreements (BAAs) can reference and build upon.

Objectives of the MDSA

1. **Standardization**: Establish uniform data sharing protocols and standards across all participating entities.
2. **Compliance**: Ensure adherence to applicable federal, state, and local laws, including HIPAA, FERPA, and state-specific privacy laws.
3. **Security**: Define security measures to protect shared data from unauthorized access and breaches.
4. **Governance**: Outline the governance structure for managing data sharing and resolving disputes.
5. **Transparency**: Provide clear guidelines on data use, access, and participant responsibilities.

Key Components of the MDSA

1. **Scope and Purpose**
    - **Scope**: Define the types of data covered by the agreement, including health, education, and social service data.
    - **Purpose**: Explain the objectives of data sharing, such as improving service coordination, enhancing care delivery, and supporting community health initiatives.
2. **Legal and Regulatory Compliance**
    - **Applicable Laws**: List the federal, state, and local laws that govern data sharing, including HIPAA, FERPA, and any relevant state privacy laws.
    - **Compliance Obligations**: Detail the obligations of each party to comply with these laws, including obtaining necessary consents and maintaining data security.
3. **Data Sharing Protocols**
    - **Data Categories**: Specify the categories of data that can be shared, such as demographic information, health records, and service utilization data.
    - **Sharing Conditions**: Define the conditions under which data can be shared, including permissible uses and restrictions.
    - **Data Quality**: Establish standards for data accuracy, completeness, and timeliness.
4. **Security Measures**
    - **Data Protection**: Outline the administrative, technical, and physical safeguards to protect shared data.
    - **Access Controls**: Define who has access to shared data and the levels of access permitted.

   - **Incident Response**: Provide procedures for responding to data breaches and other security incidents.
5. **Governance Structure**
   - **Steering Committee**: Establish a governing body responsible for overseeing the implementation and management of the MDSA.
   - **Roles and Responsibilities**: Define the roles and responsibilities of each participating entity and the steering committee.
   - **Dispute Resolution**: Outline procedures for resolving conflicts related to data sharing.
6. **Consent and Authorization**
   - **Informed Consent**: Require obtaining informed consent from individuals whose data will be shared, detailing how their data will be used and protected.
   - **Revocation of Consent**: Provide mechanisms for individuals to revoke their consent and for the cessation of data sharing upon revocation.
7. **Audit and Compliance Monitoring**
   - **Regular Audits**: Mandate regular audits to ensure compliance with the MDSA and applicable laws.
   - **Reporting Requirements**: Establish reporting requirements for data sharing activities and compliance issues.
   - **Non-Compliance Consequences**: Specify consequences for non-compliance, including termination of the agreement or other legal actions.

MDSA Implementation Steps

1. **Drafting the MDSA**
   - Collaborate with legal experts, stakeholders, and participating entities to draft the MDSA.
   - Ensure the agreement aligns with existing policies, procedures, and legal requirements.
2. **Stakeholder Engagement**
   - Engage all relevant stakeholders, including service providers, community organizations, and individuals, to review and provide input on the MDSA.
   - Address any concerns or suggestions to ensure broad support and understanding.
3. **Approval and Adoption**
   - Obtain formal approval of the MDSA from all participating entities.
   - Adopt the MDSA as the guiding framework for data sharing within the CIE.
4. **Training and Awareness**
   - Conduct training sessions for all stakeholders to ensure understanding and compliance with the MDSA.
   - Provide ongoing education and support to address any questions or issues that arise.
5. **Monitoring and Evaluation**
   - Regularly monitor the implementation of the MDSA to ensure compliance and effectiveness.
   - Evaluate the impact of data sharing on service coordination and community outcomes, making adjustments as needed.

The Master Data Sharing Agreement is a critical component of implementing a Community Information Exchange, providing a standardized and legally compliant framework for data sharing. By clearly defining the roles, responsibilities, and protocols, the MDSA fosters collaboration and trust among participating entities, ultimately enhancing service delivery and community well-being.

Sharing Data Under HIPAA

Sharing data under the Health Insurance Portability and Accountability Act (HIPAA) requires adherence to stringent rules and guidelines to ensure the confidentiality, integrity, and security of Protected Health Information (PHI). Here are the key components for compliantly sharing data under HIPAA:

1. **Understanding PHI**
    - **Definition of PHI**: PHI includes any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual.
    - **Scope of PHI**: This covers a wide range of identifiers, not just medical records.
2. **Privacy Rule Compliance**
    - **Use and Disclosure of PHI**: PHI should only be used or disclosed for treatment, payment, or healthcare operations unless patient authorization is obtained or a specific exception applies.
    - **Minimum Necessary Standard**: When PHI is disclosed, only the minimum necessary information should be shared to achieve the purpose of the disclosure.
3. **Security Rule Compliance**
    - **Administrative Safeguards**: Implement policies and procedures to manage the selection, development, implementation, and maintenance of security measures.
    - **Physical Safeguards**: Protect electronic systems, equipment, and data from physical threats.
    - **Technical Safeguards**: Use technology to control access to PHI and protect communications containing PHI transmitted electronically.
4. **Business Associate Agreements (BAAs)**
    - **Agreements with Third Parties**: Covered entities must have BAAs in place with business associates who handle PHI on their behalf.
    - **BAA Requirements**: BAAs must outline the permissible uses of PHI by the business associate and ensure that they will use appropriate safeguards.
5. **Patient Rights**
    - **Access and Amendment**: Patients have rights to access and request amendments to their PHI.
    - **Accounting of Disclosures**: Patients can request an accounting of certain types of disclosures of their PHI.
6. **Breach Notification Rule**
    - **Reporting Requirements**: Covered entities must report any breach of unsecured PHI to affected individuals, the Department of Health and Human Services (HHS), and, in some cases, the media.
7. **Training and Awareness**
    - **Staff Training**: Regular training of staff who handle PHI on HIPAA policies and procedures is crucial.
    - **Awareness**: Maintaining awareness about the evolving nature of threats to data security and updates in HIPAA regulations.
8. **Record Keeping and Documentation**
    - **Policies and Procedures Documentation**: Maintain written privacy and security policies and procedures.
    - **Compliance Records**: Keep records of privacy and security practices, including risk analyses and remediation plans.

Covered Entities

In the context of the Health Insurance Portability and Accountability Act (HIPAA), "Covered Entities" are defined as organizations or individuals that engage in certain healthcare activities and are thus subject to HIPAA's regulations. Typical examples of covered entities include:

1. **Healthcare Providers**:
    - Doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies that transmit any health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted a standard.

2. **Health Plans**:
   - Health insurance companies, HMOs (Health Maintenance Organizations), company health plans, and government programs that pay for healthcare, such as Medicare, Medicaid, and the military and veterans' healthcare programs.
3. **Healthcare Clearinghouses**:
   - Entities that process nonstandard health information they receive from another entity into a standard format or vice versa.
4. **Medicare Prescription Drug Card Sponsors**:
   - Companies that provide Medicare-approved prescription drug cards, subject to certain conditions.

Additionally, while not covered entities themselves, **Business Associates** of covered entities are also subject to certain HIPAA regulations. These can include:

- Third-party administrators that assist health plans with claims processing.
- CPAs, attorneys, and IT consultants who have access to PHI (Protected Health Information) as part of the services they provide to a covered entity.
- Billing and coding services, claims processing companies, and healthcare management services.
- Data analysis, processing, or administration services.

It's important to note that organizations can be a covered entity in one aspect of their operations but not in others. For instance, a university may have a healthcare provider component (such as a university hospital) that is a covered entity, while other parts of the university are not.

County Health and Human Services as Covered Entities

County health departments must comply with HIPAA if they are covered entities. HIPAA applies to any organization or individual that creates, receives, maintains, or transmits electronic protected health information (ePHI).

Covered entities include:

- State Medicaid programs
- Local public health departments
- Local governments that are covered entities

HIPAA's Privacy Rule recognizes the need for public health authorities to have access to protected health information to carry out their public health mission.

Non-covered Entities

Some examples of organizations that do not have to follow HIPAA include:

- Auto insurance companies
- Schools and school districts
- Law enforcement agencies
- State agencies not involved in healthcare administration or services
- Life insurers
- Employers
- Workers compensation carriers
- Many state agencies like child protective service agencies
- Many municipal offices

Requirements for the Execution of a Business Associate Agreement with Covered Entities

In the context of HIPAA compliance, a Business Associate Agreement (BAA) is often part of a broader relationship between a covered entity and a business associate (agent). While it's not strictly necessary for there to be a separate service agreement in order to sign a BAA, it is common practice for several reasons:

1. **Defining the Relationship and Scope of Services**: A service agreement typically outlines the specific services being provided by the business associate to the covered entity. This includes details on the scope of work, performance expectations, payment terms, and other operational aspects of the relationship.
2. **Compliance and Legal Requirements**: The BAA, on the other hand, is specifically focused on ensuring compliance with HIPAA's requirements regarding the use and protection of Protected Health Information (PHI). It outlines the obligations and responsibilities of the business associate in relation to the handling of PHI.
3. **Operational Clarity**: Having a service agreement in place alongside a BAA can provide clarity and prevent misunderstandings about the nature of the work, the handling of PHI, and the responsibilities of each party.
4. **Risk Management**: A service agreement can also include terms related to liability, indemnification, dispute resolution, and other legal protections for both parties.
5. **Regulatory Compliance**: Sometimes, regulations or internal policies of the covered entity might necessitate a formal service agreement in addition to a BAA.
6. **Integration of Agreements**: Often, the BAA is either attached as an addendum to the service agreement or integrated into the service agreement as a section or clause, ensuring that all aspects of the relationship are covered in a single, cohesive legal document.
7. **Flexibility for Specific Arrangements**: In some cases, particularly in smaller or less formal arrangements, the BAA might be the only written agreement between the parties. However, this is less common and generally not advisable due to the lack of detail regarding the broader scope of the relationship.

While a separate service agreement is not a legal prerequisite for a BAA under HIPAA, it is typically part of best practices to have both. This ensures a clear, comprehensive, and compliant framework for the relationship between a covered entity and a business associate. Legal counsel should be consulted to create these documents, ensuring they meet all legal requirements and adequately protect the interests of both parties.

Service Agreements and Consideration Requirements

In contract law, for an agreement to be considered legally binding, it generally must contain certain elements, one of which is often referred to as "consideration." Consideration is something of value that is exchanged between the parties to a contract. This can include money, goods, services, promises, or other types of value. Key elements of consideration include:

1. **Remuneration as Consideration**: In many contracts, remuneration (payment of money) is a common form of consideration. One party agrees to provide a service or a product, and the other party agrees to pay for that service or product.
2. **Non-Monetary Consideration**: However, consideration does not necessarily have to be monetary. It can be anything of value to the parties involved. For example, in a barter agreement, goods or services are exchanged without any money changing hands.
3. **Mutuality of Obligation**: The key aspect is that there must be a mutuality of obligation – each party is obligated to give or do something in exchange for what they receive. A unilateral promise without such an exchange is generally not enforceable as a contract.
4. **Nominal Consideration**: In some cases, contracts may include what is known as "nominal consideration" (e.g., $1) to satisfy the legal requirement for consideration, even when the actual value of the exchange is not balanced or is more symbolic.

5. **Exceptions and Specific Contexts**: There are exceptions and specific contexts where contracts might be valid without traditional consideration. For instance, certain promissory notes and charitable pledges can sometimes be enforced without consideration, depending on jurisdiction and specific circumstances.

In summary, while remuneration is a common form of consideration, it is not the only form. A legally binding service agreement must have consideration, but this consideration can take various forms, not just monetary payment. The essential factor is that something of value is exchanged between the parties.

Use of a Memorandum of Understanding (MOU) in Lieu of a Service Agreement

A Memorandum of Understanding (MOU) can sometimes be used in place of a formal service agreement, but its appropriateness and effectiveness depend on the specific circumstances and the level of detail in the MOU. In the context of sharing data between a covered entity and a business associate under HIPAA, there are several important considerations:

1. **Nature of an MOU**: An MOU is typically less formal than a service agreement. It is often used to outline the intentions of the parties and the general terms of their agreement, but it might not include the detailed terms and conditions that a formal contract would.
2. **Legal Binding Nature**: While MOUs can be legally binding if they contain all the elements of a contract (such as offer, acceptance, intention to create legal relations, and consideration), they are often viewed as expressions of understanding rather than enforceable contracts. The binding nature of an MOU depends on its content and how it is worded.
3. **Scope and Detail**: For an MOU to effectively take the place of a service agreement, it should be sufficiently detailed. This includes clearly defining the roles and responsibilities of each party, the scope of the data to be shared, the purpose of data sharing, data protection measures, compliance with HIPAA and other relevant laws, and procedures for breach notification, among other aspects.
4. **HIPAA Compliance**: Under HIPAA, covered entities must have a Business Associate Agreement (BAA) with any business associate that creates, receives, maintains, or transmits Protected Health Information (PHI) on their behalf. This is a specific requirement and an MOU, even if it covers other aspects of the relationship, may not suffice if it does not meet the criteria of a BAA.
5. **Specificity of Terms**: Service agreements usually include specific terms regarding duration, termination, dispute resolution, confidentiality, indemnification, and other legal clauses. If the MOU lacks these specifics, it may not provide the same level of clarity and protection as a service agreement.
6. **Interpretation and Enforcement**: MOUs may be open to broader interpretation than formal contracts, potentially leading to disputes or misunderstandings. The enforceability of an MOU can be a complex legal question, often requiring judicial interpretation.
7. **Legal and Regulatory Requirements**: Given the regulatory environment, especially in healthcare, it's crucial to ensure that any agreement, whether it's an MOU or a formal contract, meets all legal and regulatory requirements.

In summary, while an MOU can sometimes serve the purpose of a service agreement, it's important to carefully consider whether it includes all necessary details and legal requirements, especially in a regulated environment like healthcare. In many cases, particularly where HIPAA compliance is concerned, a more formal service agreement and a separate BAA might be necessary to fully address all legal obligations and ensure enforceability.

Sufficiency of a BAA vs. Data Sharing Agreement

In the context of HIPAA compliance, whether a Business Associate Agreement (BAA) suffices to support the transmission of data to an agent or if an additional data-sharing agreement is needed depends on the specifics of the relationship between the covered entity and the business associate, as well as the nature of the data being shared. Here are key points to consider:

Business Associate Agreement (BAA)

- **Primary Purpose**: The BAA is specifically designed to meet HIPAA requirements. It establishes the permissible uses and disclosures of Protected Health Information (PHI) by the business associate, as mandated by HIPAA.
- **Contents**: A BAA typically includes terms that cover the use, safeguarding, and disclosure of PHI, as well as requirements for reporting breaches of unsecured PHI.
- **Legally Required**: For any entity that functions as a business associate, a BAA is a legal requirement under HIPAA.

Data Sharing Agreement (DSA)

- **Additional Specifics**: A DSA can provide more detailed provisions regarding the handling, processing, and management of data that may not be specifically related to PHI or covered under HIPAA.
- **Scope**: DSAs may cover broader types of data and additional obligations such as data quality, data retention, and data destruction policies, which might not be extensively detailed in a BAA.
- **Context-Specific Requirements**: In certain contexts, a DSA might be necessary to address specific requirements of a project or collaboration that are not fully covered in a BAA.

Deciding Between BAA and DSA

1. **Nature of Data**: If the data being shared is exclusively PHI and the relationship is covered under HIPAA, a BAA may suffice.
2. **Additional Data Types**: If the business associate will handle other types of data beyond PHI, or if there are specific requirements or risks associated with the data sharing that are not addressed in the BAA, a separate DSA may be necessary.
3. **Compliance with Other Laws**: If other laws and regulations apply to the data (such as FERPA for educational records or CCPA for consumer data in California), a DSA may be needed to ensure compliance with those regulations.
4. **Complex Projects**: For more complex arrangements or projects that involve multiple types of data, a DSA can provide the necessary legal framework to address all aspects of data handling and sharing.

While a BAA is essential for HIPAA compliance, whether an additional DSA is required depends on the nature of the data shared and the specifics of the relationship. A BAA might suffice in many cases, but a DSA can be beneficial or necessary in situations involving a broader scope of data or specific project requirements. Legal advice should be sought to ensure appropriate and compliant data sharing arrangements.
Sharing Data Under FERPA

Key Components of Data Sharing Agreements Under FERPA

- **Purpose of Data Sharing**: Clearly define why the data is needed and how it will be used.
- **Confidentiality and Privacy**: Include clauses that ensure the protection of student data, consistent with FERPA requirements.
- **Access Controls**: Stipulate who can access the data and under what circumstances.
- **Data Retention and Destruction**: Define how long the data can be retained and the process for securely destroying the data when it's no longer needed.
- **Parental Consent**: If applicable, include procedures for obtaining parental consent.
- **Audit and Compliance**: Provision for regular audits to ensure compliance with the agreement and FERPA.

Considerations for Specific Data Types

- **Directory Information**: Understand what constitutes directory information, which can be shared more freely under FERPA.
- **Non-directory Information**: Requires stricter controls and often explicit consent for sharing.

State and Local Regulations

- Be aware of any additional state or local regulations that may apply to student data privacy beyond FERPA.

Consultation with Legal Counsel

- Given the complexity and potential legal ramifications, it's crucial to work with legal counsel experienced in education law to draft or review any agreements.

Training and Compliance

- Ensure that all personnel who will handle the data are trained in FERPA compliance and understand the obligations under the agreement.

Operating as a School Official

Operating as a school official for a Local Education Agency (LEA) involves various legal and administrative considerations, particularly when it comes to accessing and handling student records under the Family Educational Rights and Privacy Act (FERPA). For a third-party, the necessity of an executed Service Agreement, or similar legal document, which defines the business relationship between LEA and agent is typically required but depends on several factors:

1. **Role and Responsibilities**
    - **Definition of a School Official**: FERPA defines a school official as a person employed by the LEA as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel); a person serving on the school board; a person or company with whom the LEA has contracted to perform a special task (such as an attorney, auditor, medical consultant, or therapist); or a parent or student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.
    - **Determination of "Legitimate Educational Interest"**: A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.
2. **Service Agreement or Contractual Relationship**
    - For external parties (not directly employed by the LEA) who operate as school officials, a formal agreement or contract is typically necessary.
    - This agreement should outline the nature of the service being provided, the responsibilities and expectations of the school official, and compliance requirements with FERPA.
3. **FERPA Compliance**
    - Any school official, whether internal or external, must comply with FERPA's requirements regarding the protection of student education records.
    - The agreement or contract should stipulate adherence to FERPA’s privacy and data security standards.
4. **Access to Education Records**
    - The agreement should specify the extent to which the school official has access to education records, consistent with their role and responsibilities.
    - Access should be limited to what is necessary for the performance of their duties.
5. **Data Security and Confidentiality**

- The agreement should include provisions for ensuring the confidentiality and security of education records.
- Policies regarding data breach notification should also be included.

6. **Duration and Scope**
   - It should clearly state the duration of the agreement and the specific scope of services being provided.
7. **Legal and Ethical Considerations**
   - If the school official is handling sensitive or personal information, there may be additional legal and ethical considerations to address in the agreement.
8. **Review and Approval**
   - Such agreements should be reviewed and approved by the LEA's legal counsel to ensure compliance with all applicable laws and regulations.

Recordation: FERPA (§ 99.32(d)(2)) does not require educational agencies and institutions to record disclosures of PII from education records to school officials under § 99.31(a)(1).

In summary, while internal school officials (such as employees of the LEA) may not need a separate service agreement to perform their roles, external parties acting as school officials typically require a formal agreement or contract. This agreement should detail their role, responsibilities, and the scope of access to education records, and ensure compliance with FERPA and other relevant laws. Legal consultation is recommended to ensure these agreements meet all necessary legal standards.

Public Disclosure of FERPA data

"Disclosure" means to permit access to or the release, transfer, or other communication of PII by any means. Disclosure can be authorized, such as when a parent or an eligible student gives written consent to share education records with an authorized party or if the disclosure meets one or more of the conditions outlined in 20 U.S.C. § 1232g(b) and (h) – (j) and 34 CFR § 99.31. Disclosure can also be unauthorized or accidental.

An unauthorized disclosure can happen due to a data breach or a loss.

An accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individual students to be identified. "Disclosure avoidance" refers to the efforts made to reduce the risk of disclosure, such as applying statistical methods to protect PII in aggregate data tables. These safeguards, often referred to as disclosure avoidance methods, can take many forms (e.g., data suppression, rounding, recoding, etc.).

Standard to evaluate accidental disclosure risk

The FERPA standard for de-identification assesses whether a "reasonable person in the school community who does not have personal knowledge of the relevant circumstances" could identify individual students based on reasonably available information, including other public information released by an agency, such as a report presenting detailed data in tables with small size cells (34 CFR §99.3 and §99.31(b)(1)). The "reasonable person" standard should be used by State and local educational agencies and institutions to determine whether statistical information or records have been sufficiently redacted prior to release such that a "reasonable person" (i.e., a hypothetical, rational, prudent, average individual) in the school community should not be able to identify a student because of some well-publicized event, communications, or other similar factor. School officials, including teachers, administrators, coaches, and volunteers, are not considered in making the reasonable person determination since they are presumed to have inside knowledge of the relevant circumstances and of the identity of the students.

Best practices in avoiding accidental disclosure

Commonly used disclosure avoidance methods include data suppression, blurring, and perturbation. When deciding which method to apply in a specific situation, it is important to evaluate the different methods in terms of their effects on the utility of the data and the risk of disclosure.

- Suppression involves removing data (e.g., from a cell or a row in a table) to prevent the identification of individuals in small groups or those with unique characteristics. This method may often result in very little data being produced for small populations, and it usually requires additional suppression of non-sensitive data to ensure adequate protection of PII (e.g., complementary suppression of one or more non-sensitive cells in a table so that the values of the suppressed cells may not be calculated by subtracting the reported values from the row and column totals). Correct application of this technique generally results in low risk of disclosure; however, it can be difficult to perform properly because of the necessary calculations (especially for large multi-dimensional tables). Further, if additional information related to the suppressed data is available elsewhere, the suppressed cells may potentially be re-calculated.
- Blurring is used to reduce the precision of the disclosed data to minimize the certainty of identification. Examples of blurring include rounding, aggregating across different populations or geographies, and reporting percentages and ranges instead of exact counts. This method may affect the utility of the data by reducing users' ability to make inferences about small changes in the data. Similarly, blurring methods that rely on aggregation across geographies or subgroups may interfere with time-series or cross-sectional data analysis. Applying this technique generally ensures low risk of disclosure; however, if any un-blurred cell counts or row and/or column totals are published (or are available elsewhere), it may be possible to calculate the values of sensitive cells.
- Perturbation involves making small changes to the data to prevent identification of individuals from unique or rare population groups. Examples of this technique include swapping data among individual cells (this still preserves the marginal distributions, such as row totals) and introducing "noise," or errors (e.g., by randomly reclassifying values of a categorical variable). This method helps to minimize the loss of data utility as compared to other methods (e.g., compared to the complete loss of information due to suppression); however, it also reduces the transparency and credibility of the data. Therefore, perturbation is often considered inappropriate for public reporting of program data, from an accountability perspective. Applying this technique generally ensures low risk of disclosure, as long as the rules used to alter the data (e.g., the swapping rate) are protected. This requires securing the information about the technique itself as well as restricting access to the original data, so that perturbation rules cannot be reverse-engineered.

Use of small cells when displaying data

Reporting unrounded frequency counts in small cells, such as an exact number of students in a small group, does not by itself constitute a disclosure; however, the smaller the cell size, the greater the likelihood that someone might be able to identify an individual within that cell, and thus the greater the risk of disclosure. Many statisticians consider a cell size of 3 to be the absolute minimum needed to prevent disclosure, though larger minimums (e.g., 5 or 10) may be used to further mitigate disclosure risk (see below).

U.S. Department of Education recommendations for disclosure avoidance

The Department does not mandate a particular method, nor does it establish a particular threshold for what constitutes sufficient disclosure avoidance. These decisions are left up to the individual State and local educational agencies and institutions to determine what works best within their specific contexts. As a general recommendation, in aggregate publicly available reports, whenever possible, data about individual students (e.g., proficiency rates presented as cross-tabulated tables) should be combined with data from a sufficient number of other students to disguise the attributes of a single student. When this is not possible, data about small numbers of students should not be published. Moreover, under the ESEA, each State must establish a minimum sub-group size (e.g., number of students in a table cell) below which it will not publicly report assessment data. This threshold value and other reporting rules should be specified in the documents describing the State's data reporting policies and practices implemented to protect student privacy. Minimum cell sizes adopted by the States range from 5 to 30 students, with a majority of States using 10 as their minimum (NCES 2011-603). Please note that simple suppression of small subgroups may not be sufficient to protect the privacy of all students, since the suppressed numbers can often be easily calculated by subtracting the reported subgroups' totals from the all-student totals or by comparing the school and district enrollment information. In some cases, complementary suppression of additional non-sensitive cells may be necessary.

The Department strongly suggests using a computer software or algorithm to apply disclosure limitation methods, as some techniques may be difficult to implement accurately by hand. In particular, to ensure correct application of data suppression method, care should be taken when suppressing any complementary cells. Lastly, it is preferable, from a data user perspective, to apply consistent methods year to year and to use the same disclosure avoidance strategies for similar types of data releases.

Additional Resources

- Case Study #5: Minimizing Access to PII: Best Practices for Access Controls and Disclosure Avoidance Techniques. Privacy Technical Assistance Center (Oct 2012): http://ptac.ed.gov/sites/default/files/case-study5-minimizing-PII-access.pdf
- Code of Federal Regulations - Title 34: Education. Disaggregation of data. 34 CFR §200.7: www.gpo.gov/fdsys/pkg/CFR-2011-title34-vol1/pdf/CFR-2011-title34-vol1-sec200-7.pdf
- FERPA regulations, U.S. Department of Education: www.ed.gov/policy/gen/reg/ferpa FERPA regulations amendment. U.S. Department of Education (December 9, 2008): www.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf
- FERPA regulations amendment. U.S. Department of Education (December 2, 2011): www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf
- Frequently Asked Questions—Disclosure Avoidance. Privacy Technical Assistance Center (Oct 2012): http://ptac.ed.gov/sites/default/files/FAQs_disclosure_avoidance.pdf
- Privacy Technical Assistance Center (PTAC), U.S. Department of Education: http://ptac.ed.gov
- SLDS Technical Brief 3: Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (NCES 2011-603): http://nces.ed.gov/pubs2011/2011603.pdf
- Statistical Policy Working Paper 22 - Report on Statistical Disclosure Limitation Methodology. Federal Committee on Statistical Methodology, Office of Management and Budget (1994): http://fcsm.gov/working-papers/wp22.html
- Technical Brief: Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (NCES 2011-603): http://nces.ed.gov/pubs2011/2011603.pdf
- Statistical Policy Working Paper 22 - Report on Statistical Disclosure Limitation Methodology. Federal Committee on Statistical Methodology, Office of Management and Budget (1994): http://fcsm.gov/working-papers/wp22.html
- Technical Brief: Statistical Methods for Protecting Personally Identifiable Information in the Disclosure of Graduation Rates of First-Time, Full-Time Degree- or Certificate-Seeking Undergraduate Students by 2-

Year Degree-Granting Institutions of Higher Education (NCES 2012- 151): http://nces.ed.gov/pubs2012/2012151.pdf

Potential Legal Framework for Education Record Disclosure – Demonstration of Legitimate Educational Interest

Overview

For a Local Education Agency (LEA) to share pupil records with a technical vendor, there must be legitimate educational interest that supports the disclosure. To demonstrate this, a vendor must clearly show that their services support the educational or administrative functions of the LEA. This is primarily achieved through a detailed written agreement that specifies the nature of the services, the educational purposes they serve, and strict data use and security protocols. By adhering to these requirements, vendors can align with FERPA and the California Education Code, ensuring that they operate in the educational interest of students.

Definition of Legitimate Educational Interest

FERPA

FERPA defines "legitimate educational interest" as the need for a school official to review an education record in order to fulfill their professional responsibilities. According to 34 CFR § 99.31(a)(1)(i)(B):

- A contractor, consultant, volunteer, or other party to whom an educational institution has outsourced institutional services or functions may be considered a "school official" with legitimate educational interest, provided that the contractor:
  - Performs an institutional service or function for which the school would otherwise use employees.
  - Is under the direct control of the school with respect to the use and maintenance of education records.
  - Uses education records only for authorized purposes and does not redisclose the information without proper consent.

California Education Code

The California Education Code § 49076 (a)(2)(G)(i) outlines similar provisions, emphasizing that contractors or consultants must:

- A contractor or consultant with a legitimate educational interest who has a formal written agreement or contract with the school district regarding the provision of outsourced institutional services or functions by the contractor or consultant.

Demonstrating Legitimate Educational Interest

For a vendor providing technology services, demonstrating legitimate educational interest involves ensuring that the services provided directly support the educational mission and administrative functions of the LEA. In order to achieve this, practical steps should include:

1. **Written Agreement:**
   - The LEA must have a detailed written contract with the vendor. This agreement should specify:
     - The exact nature of the services provided.
     - How these services support the educational and/or administrative functions of the LEA.
     - The vendor’s responsibilities in terms of data use, security, and confidentiality.
2. **Data Use Policies:**
   - The vendor must use the data solely for the purposes outlined in the contract and must implement strict data security measures.

- The vendor should not use the data for any commercial purposes, such as targeted advertising or creating student profiles for non-educational purposes.

3. **Direct Control:**
   - The LEA must maintain direct control over the vendor's access to and use of student data. This can include provisions for:
     - Regular audits and monitoring.
     - Clear protocols for data access and handling.
     - Immediate notification of any data breaches.

Examples in Practice

1. **Learning Management Systems (LMS):**
   - Vendors like Canvas, Google Classroom, and Blackboard provide platforms that allow teachers to manage coursework, track student progress, and facilitate online learning. These platforms are directly tied to the instructional process and help schools achieve their educational objectives.
2. **Student Information Systems (SIS):**
   - Companies like PowerSchool and Infinite Campus provide systems for managing student records, attendance, grades, and other administrative functions. These systems are crucial for school administration and directly support the management of student data.
3. **Assessment Tools:**
   - Tools like i-Ready and NWEA MAP provide assessment services that help schools measure student progress and identify areas for improvement. These assessments are integral to the educational process and support data-driven decision-making in schools.

Demonstrating Legitimate Educational Interest for Technical Development of the Fresno CIE Suicide Prevention Pilot

Conceptual Framework for Fresno CIE Vendor Statement of Service for the Suicide Prevention Pilot

A vendor will provide services to the Local Education Agency (LEA) that involves securely hosting student IDs. These IDs will only be used to send alerts containing these student IDs to the LEA which submitted them in the event of a match with a 5150 hold or similar event logged within a healthcare setting. The data will be securely held solely for this purpose and will remain under the direct contractual control of the LEA. Services support the LEA’s educational and administrative functions by enabling timely intervention and support for students experiencing traumatic events.

Elements of Legitimate Educational Benefit through the LEA

- **Timely Response:**
  - The school can quickly mobilize counseling services, contact the student’s family, and offer other necessary supports, helping to address the student’s needs effectively.
- **Targeted Support:**
  - By receiving real-time alerts, the school can tailor its response to the specific situation, ensuring the student gets the appropriate help.

Legal and Practical Justifications

- **Emergency Situations:**
  - FERPA allows schools to share student records without consent in health or safety emergencies. While this service primarily uses the "legitimate educational interest" rule, the urgent nature of a 5150 hold highlights the need for quick information sharing to protect the student.
- **Supporting Student Health:**
  - The California Education Code supports sharing information necessary to protect a student’s health and safety. The vendor’s role in providing real-time alerts fits within this protective scope,

helping the school ensure the student’s well-being.

Relevant Legal Requirements and Justification
Federal Law: FERPA
The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. According to FERPA, schools can share student records with outside parties, like vendors, under certain conditions:

1. **Necessary Services:**
   - The vendor must provide a service that the school would otherwise perform using its own staff. In this case, the service is hosting student IDs in order to provide alerts about mental health crises, which supports the school's responsibility to care for student welfare.
2. **Control and Use:**
   - The school must have direct control over the vendor regarding how the student records are used and maintained. This means the school sets strict rules about what the vendor can do with the information.
3. **Purpose Limitation:**
   - The vendor can only use the student records for the specific purpose outlined in their agreement with the school, which is to provide a student ID to participating LEAs after generating real-time alerts for 5150 holds and not for any other purpose.

State Law: California Education Code
The California Education Code has similar requirements to FERPA:

1. **Written Agreement:**
   - There must be a formal contract between the school district and the vendor specifying the service to be provided, which in this case is generating alerts for LEAs to use during a student mental health crises.
2. **Educational Interest:**
   - The vendor’s service must clearly support the educational mission. By providing timely alerts, the school can quickly offer necessary support, helping the student stay on track academically despite the crisis.
3. **Data Security:**
   - The vendor must implement strong security measures to protect student information from unauthorized access or disclosure. This includes measures like encryption and regular security audits.

Summary Conclusion

The collaboration between a school district and a vendor to host student IDs and provide real-time alerts for mental health crises complies with both federal and state laws. By ensuring the vendor operates under the school’s control, uses data only for its intended purpose, and protects the information with robust security measures, the arrangement helps schools support their students during critical times while adhering to legal requirements. This integration of technology into school services highlights a practical way to enhance student support and well-being.
The

FCSS Legal Review Summary of Sharing School Data with the CIE

The primary legal consideration in sharing data with the CIE is whether submission of student ID numbers and gender information for suicide prevention alerts or other purposes yet to be determined aligns with the concepts of “legitimate educational interest” and “outsourced institutional functions” under FERPA and California Education Code.

The main legal challenge lies in whether an HIE (Health Information Exchange) hosting student data to provide alerts on suicide-related events can be seen as fulfilling an LEA function that would typically require LEA employees. This issue hinges on whether such alerts fall under educational functions or more accurately represent behavioral health interests, which do not clearly fit FERPA’s framework for “legitimate educational interest” or ”outsourced institutional functions.” This limits data sharing from educational sources into a CIE environment to directory information only.

FERPA’s “emergency” exception is another example of a legal portal for sharing data, but is limited to ex post facto applications, leaving gaps for ongoing data sharing without specific emergencies.

A legally viable approach for educational partners participation in the CIE is to use directory information, which falls outside FERPA’s “education records” and the California Education Code’s “pupil records.” With directory information, LEAs can confirm student identity and residence without needing to apply “legitimate educational interest” or “outsourced institutional function” arguments. This would enable data sharing within legal bounds, avoiding the complexities of FERPA and Education Code requirements.

Key Recommendations for the Project:

1. **Use of Directory Information:** Instead of unique student IDs, directory information could confirm student identity and district residency, serving the intended function without invoking FERPA or California Education Code privacy restrictions.

This approach aims to balance legal compliance with the operational goals of the Fresno CIE Suicide Prevention Pilot while minimizing potential regulatory obstacles for participating LEAs.

Service Level Agreements (SLAs) or Data Sharing Agreements (DSAs)

SLAs and DSAs are needed between any parties needing to share sensitive data. Work is needed to identify specific SLA's and DSA's for entities involved in sharing of data for this effort as some do not currently exist or if agreements exist, they are not sufficient to cover the needed scope of requirements. Samples of considerations regarding, and elements of, SLAs and DSAs (including consent and privacy considerations), include:

SLA:

- Business objectives
- Performance standards
- Reporting mechanisms
- Critical failure processes
- Change processes
- Uptime/Availability
- Time to recovery and response
- Continuity of services
- Disaster recovery/failover

DSA:

- Authority
- Access provisions
- Confidentiality & disclaimers
- Timeframe for agreement
- Authorized use and disclosure
- Data retention and disposal

Example Industry Standard SLAs

Amazon Web Services (AWS)

- **Link:** AWS Service Level Agreement
- **Overview:**
  - **Service Availability:** AWS guarantees a monthly uptime percentage of at least 99.99% for most of its services, including EC2 (Elastic Compute Cloud) and S3 (Simple Storage Service).
  - **Performance Metrics:** AWS defines performance metrics for various services, ensuring predictable and reliable performance levels.
  - **Compensation:** In the event of service outages or performance degradation, AWS offers service credits as compensation, which can be used to offset future bills.

Microsoft Azure

- **Link:** Microsoft Azure SLA
- **Overview:**
  - **Service Availability:** Azure provides a 99.9% uptime guarantee for most of its services, with some services offering up to 99.99% availability.
  - **Downtime Definition:** Clear definitions of what constitutes downtime, including planned maintenance windows and unplanned service interruptions.
  - **Service Credits:** Similar to AWS, Azure offers service credits based on the percentage of uptime achieved in a billing month.

Recommended SLAs for CIE Launch

In the initial phase of the project, it is advisable to focus on a limited number of easily understood and measurable metrics. As the system evolves and its performance becomes more predictable, the SLA terms can be expanded and refined to include more detailed content and expectations. The following recommendations are based on industry norms and professional experience. Final metrics and SLAs should be developed with input from end-user stakeholders to ensure they align with user expectations for the CIE's performance.

1. Uptime Requirements

- **System Uptime:** Ensure the CIE system and individual microservices maintain a high level of availability.
    - **Suggested SLA Level:** 99.9% uptime over a week (Monday to Sunday).
    - **Methodology:** Uptime is often measured as a percentage of total available minutes. For example, with a 99.9% SLA, the CIE can have a maximum of 45 minutes of downtime per month (44,640 minutes in a 31-day month).

2. Sustainable Usage Estimates

- **Performance Metrics:** Establish baseline values for sustainable usage without significant performance degradation, including average and peak requests per second/minute for the CIE system and individual microservices.
    - **Peak Traffic/Hour Calculation:** Aggregate peak user activity from all partner organizations over the last 12 months, adding 25% to accommodate growth.
    - **Average Traffic/Hour Calculation:** Calculate the average user activity over the last three months, dividing the total by the number of systems and adding 25% for growth.

3. System Latency

- **Latency Definition:** Measure the time taken for a request to travel through the CIE microsystems, starting and ending with the API service.
    - **Current Status:** Initial latency metrics will be established post-build, following a series of load tests simulating real-world traffic.
    - **Load Testing:** Conduct load tests to simulate realistic payloads, volume, and velocity, and plan for future growth over three years.
    - **Performance Optimization:** Use load test results and logging data to identify and address performance bottlenecks, such as software bugs or inefficient architectural choices.
- **Latency Metrics:**
    - **Average Latency:** Set based on the 50-60% level of the final load test results.
    - **Maximum Latency:** Set at no more than 95% of the maximum latency observed during the final load test, subject to partner discussions.

4. Support SLAs

- **Error Severity Classifications:**
    - **Severity Level 1:** Critical Impact/System Down (complete microservice outage).
    - **Severity Level 2:** Significant Impact/Severe service degradation.
    - **Severity Level 3:** Minor Impact/Most of the microservice functions properly.
    - **Severity Level 4:** Low Impact/Informational.
- **Support Systems:**
    - **On-Call Support Paging Service:** Utilize a third-party system (e.g., PagerDuty, Incident.io) for immediate communication with on-call engineers via phone, SMS, instant messaging, or email for Severity 1 or 2 issues.
    - **Support Ticketing System:** Implement a system (e.g., Zendesk, Zoho Desk) for end users to create support tickets, facilitating two-way communication and tracking resolution times.
- **Response Times:**
    - **Severity 1 Issues:** < 15 minutes for acknowledgment by on-call engineer.
    - **Severity 2 Issues:** < 30 minutes for acknowledgment by on-call engineer.
    - **Severity 3 Issues:** < 24 hours (business day) for acknowledgment by support engineer.
    - **Severity 4 Issues:** < 5 business days for acknowledgment by support engineer.

Establishing clear SLAs is essential for ensuring the reliability and performance of the CIE. These agreements set expectations for system availability, performance, and support, helping to maintain trust and satisfaction among all stakeholders. By starting with foundational metrics and expanding them as the system matures, the CIE can continuously improve its service quality and responsiveness.

Fresno County CIE Governance Framework

High-level governance of the Fresno County Community Information Exchange (CIE) will be developed in tandem with the Technical and Operational Plan as a distinct but aligned process. Governance of the CIE is a foundational aspect critical to its success and sustainability. Effective governance ensures that the CIE operates in a manner that is transparent, inclusive, and accountable to the community it serves. This section outlines the steps necessary to establish a robust governance framework that will guide the operations and evolution of the CIE, addressing the following key areas:

1. **Identify and Define Core Governance Principles** Establishing core governance principles is essential for setting the tone and direction of the Fresno CIE. These principles will prioritize community needs, ensuring that the CIE operates transparently, inclusively, and with a strong sense of accountability. By clearly defining these principles, the CIE can build a foundation that aligns with its mission and values, fostering trust and collaboration among all stakeholders.
2. **Establish a Customized Governance Framework** The governance framework for the CIE must be tailored to address the unique needs and priorities of the Fresno community. This involves developing a structure that accommodates local dynamics and stakeholder expectations. A customized governance framework will ensure that the CIE is responsive and adaptable, providing a solid structure for decision-making and operational management.
3. **Representative Joint Governance Team** A key component of the governance framework is the establishment of a Joint Governance Team. This team will be composed of representatives from various organizations that share data and utilize the CIE. By involving diverse stakeholders in the governance process, the CIE can ensure that multiple perspectives are considered, promoting fairness and inclusivity in its operations.
4. **Conflict Resolution Mechanisms** Effective governance requires clear mechanisms for resolving conflicts that may arise between CIE partners. Establishing well-defined conflict resolution processes will help maintain harmony and collaboration within the CIE. These mechanisms should be transparent and equitable, ensuring that all parties have a fair opportunity to present their concerns and reach mutually agreeable solutions.
5. **Data Stewardship and Privacy** The governance model of the CIE must prioritize data stewardship and privacy, particularly concerning Personally Identifiable Information (PII) and Protected Health Information (PHI). Implementing stringent data protection measures will safeguard the privacy of individuals and maintain the integrity of the CIE. This commitment to data stewardship will build trust among participants and encourage broader participation in the CIE.
6. **Legal and Regulatory Compliance** Ensuring compliance with legal and regulatory requirements is crucial for the CIE's credibility and functionality. The governance framework must include mechanisms to monitor adherence to data sharing frameworks, policies, procedures, and guidelines. Additionally, it should outline processes for addressing breaches or noncompliance to protect the interests of all CIE participants and maintain the system's integrity.
7. **Regular Governance Review and Adaptation** Governance practices must evolve to remain effective and relevant. Implementing a process for regular review and adaptation of governance practices will ensure that the CIE continues to meet the changing needs of its participants and the community. Continuous improvement efforts will help the CIE stay aligned with best practices and emerging trends in data governance and community information exchange.

Overview of Fresno CIE Field-Level Governance

The Fresno Community Information Exchange (CIE) is a framework designed to enable secure and efficient data sharing among various organizations in Fresno at the field level. This governance structure ensures that each partner in the network can share and receive specific data fields according to agreed-upon rules and protocols, tailored to the specific needs and regulations of the Fresno CIE partnership. Field-level governance is essential for maintaining data privacy, compliance, and the integrity of the information exchanged within the CIE network.

Field Sharing and Partner Agreements

- **Field Sharing Decisions**: Partners in the Fresno CIE must decide which data fields they will share with other organizations. This process requires careful consideration:
  - Fields may be shared only with specific partners.
  - Certain fields may be shared with all partners in the system.
- **Internal Governance Agreements**: Each organization must establish internal governance policies to determine what data can be shared. This involves creating rules and protocols within their own governance structure to ensure data privacy and compliance with relevant regulations and organizational needs.
- **Inter-Organizational Agreements**: In addition to internal policies, organizations must agree on data sharing terms with other partners in the Fresno CIE network. These agreements define:
  - What data will be shared.
  - With whom the data will be shared.
  - The conditions under which the data can be accessed and used.
  - The frequency with which data will be shared.
  - Other parameters as defined by the partnership.

Governance for Changing Fields and Access

- **Regular Reviews and Updates**: Governance rules and data sharing agreements should be reviewed regularly to ensure they remain relevant and effective.
- **Approval Processes**: Any changes to field sharing rules must go through a formal approval process within each organization’s governance structure.
- **Technical Implementation**: Once approved, changes must be implemented technically to reflect the new rules. This involves updating data access rules, data maps, and payload configurations within the CIE system.

Technical Change Management

- **Implementing Governance Changes**: After governance decisions are made, technical teams must update the system to reflect these changes. This includes:
  - Adjusting data access rules to align with new agreements.
  - Updating data maps to ensure fields are correctly shared and received.
  - Modifying payload configurations to match the new field-sharing decisions.
- **Data Quality and Timeliness**: It is crucial to negotiate parameters such as data timeliness and quality:
  - **Timeliness of Data**: Establishing standards for how quickly data should be shared and updated in the system.
  - **Data Quality**: Ensuring that the data being shared meets agreed-upon quality standards to be useful and reliable for all partners.

- **System Testing and Validation**: Before deploying changes, thorough testing and validation are required to ensure that the new configurations work as intended and do not disrupt existing operations.

Technical Process Overview

The system will initiate a DTS process by:

- **Checking Data Access Rules**: Reviewing the data access rules per Org_ID that govern which organizations accept what data from which other organizations. While a long-term goal is full CIE data model integration between participating organizations, there should be room for self-determination for each organization regarding what information they decide to accept. For example:
  - **Organization A**: Acts as the definitive source of specific data for other organizations but does not ingest data in return. When a record is pushed into the CIE by Organization A, it goes to all other organizations. However, when others push data, the data accessibility rules within the DTS disallow any payload creation for Organization A.
    - If Organization A decides in the future to consume information from another organization, Organization C, which acts as the definitive source of a different set of data, the data access rules can be updated to reflect that Organization A will be added to the DTS payload generation if the payload comes from Organization C.
- **Finding Appropriate Data Maps**: Identifying the data map per Org_ID that accepts the payload from the system of origin. This supplies a blueprint for which payload fields that organization will accept, their equivalent field name within the organization's data structure, and any additional, relevant information required.
- **Returning the DTS Payload**: The DTS payload is returned to the TMJQ.
- **Updating the Master Record**: If this is a new client record, upon receiving the DTS payload, the TMJQ sends an update to the MPI contained within the RMS. This update reflects which organizations have the client within their systems and what their matching fields are based on the DTS-generated payload.

Importance of Fresno CIE Field-level Governance

Effective governance in the Fresno CIE ensures that data sharing is conducted in a controlled, secure, and transparent manner. It allows organizations to collaborate and benefit from shared data while maintaining control over their information. By establishing clear governance structures and robust technical processes, the Fresno CIE network can enhance its data exchange capabilities and support improved outcomes for the communities it serves.

Regularly negotiating key parameters such as data timeliness and quality allows the Fresno CIE to maintain high standards and provide timely, accurate information to all participating organizations. This structured approach ensures that the CIE adapts to changing needs and continues to serve its purpose effectively.

Maintenance and Operations Costs

Maintenance and operations costs cannot be determined until systems are architected, infrastructure is determined, vendors are selected, and support for these components are defined. Future processes will identify where the maintenance and operational costs would exist and, when possible, estimate the associated costs with the specific technology solutions and platforms identified to meet all requirements.

Data Analytics & Performance Metrics to be Required by System

System KPIs and other metrics will be established by the primary identified decisioning body for the CIE.

Risks and Mitigation

Risks and mitigation strategies must be designed by the Core Team and Workgroups once final technical requirements have been developed.

Identified Limitations to the Technical and Operational Plan

At present, there are several gaps and uncertainties regarding the technical solutions needed to support implementation.

Uncertainties Regarding Systems of Origin

Additional business requirements and the overall conceptual plans are needed to support the integration of data into the CIE.

Cross-System Analyses Needed

Data profiling analysis is needed to review the systems and understand what data will be shared in of CIE development and support the accompanying governance and legal frameworks

Summary and Next Steps

Summary

The Draft Plan describes and summarizes what is known and what additional information is needed regarding the technology and platforms required to implement integrated data to support the goals of Fresno CIE

The Draft Plan identifies:

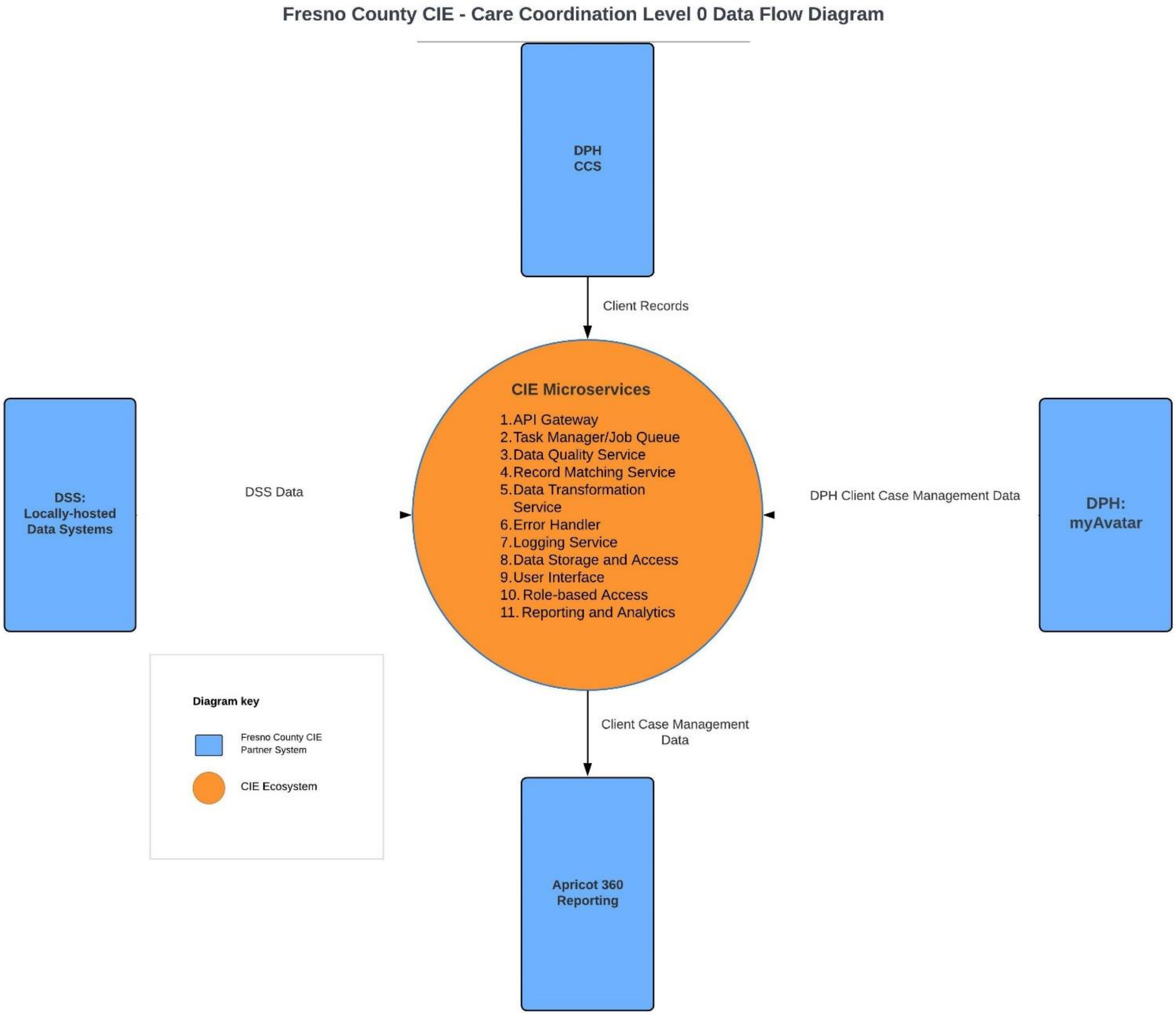
- Key systems and the need to further specify the technical features and requirements to implement integration;
- Some of the potential roles for various system users;
- The need to specify privacy issues, considerations and requirements that would apply to each of the systems and the various system users;
- Data management considerations related to the various systems; and
- Areas in which additional information is needed to create the Final Technical and Operational Plan.

Next Steps

Additional work is needed to create the Final Technical and Operational Plan, which will be gathered from key stakeholders throughout the Fresno CIE system. This information will be used to describe the technology and platforms requirements, including operational challenges in implementing the systems needed.

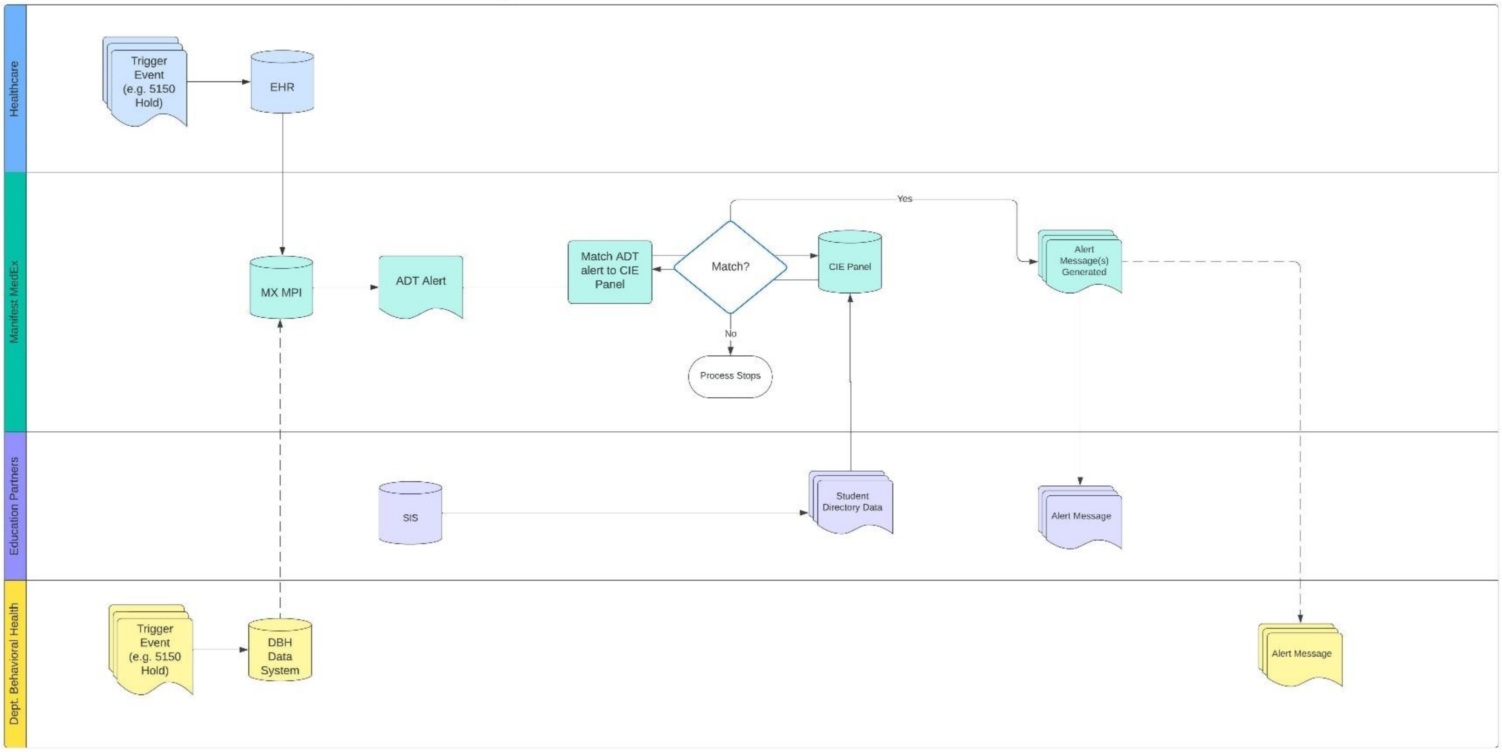
Appendix A: Fresno CIE Data Flow Mapping

Home Visitation


Fresno County CIE - Care Coordination Level 0 Data Flow Diagram
DPH
CCS
Client Records
CIE Microservices
1. API Gateway
2. Task Manager/Job Queue
3. Data Quality Service
4. Record Matching Service
5. Data Transformation Service
6. Error Handler
7. Logging Service
8. Data Storage and Access
9. User Interface
10. Role-based Access
11. Reporting and Analytics
DSS:
Locally-hosted
Data Systems
DSS Data
DPH Client Case Management Data
DPH:
myAvatar
Client Case Management Data
Apricot 360
Reporting
Diagram key
Fresno County CIE Partner System
CIE Ecosystem

Suicide Prevention

Fresno CIE Suicide Prevention Pilot - Data Flow Diagram Level 1



Appendix B: Fresno CIE Data Profiles and Analysis

This content is pending the execution of required data sharing agreements to perform the data profiling.

Appendix C: Fresno CIE Data Models

This content is pending the execution of required data sharing agreements to perform the data profiling.

Appendix D: Fresno CIE Key Questions Inventory

Why do key stakeholders want a Community Information Exchange?

- To connect sectors, to share information across various organizations to better serve students and their families.
- Real-time CIE that can serve the whole person, enhance quality of life, and aid the connections to resources/services. Increase prevention and response to SDOH needs that impact both individual and community. CIE will help us understand urgent and long-term community needs.

Why do participating partners want a Community Information Exchange?

- Improve services, systems, and practices. Build stronger communities. Build more equitable resource allocation, access, and outcomes.

What are the key success criteria for the Community Information Exchange?

- Meeting the requirements of partners/stakeholders, staying on budget and timeline, finding and agreeing on a platform that can provide integration and interoperability across systems, commitment from partners, and alignment of existing county and community efforts.

Who does the Community Information Exchange primarily serve? .

- The CIE serves providers/partners (social services sector and healthcare sector) whose primary use of the CIE is to enhance their response, services, resources, and care coordination for both individual and community. Anyone who needs the CIE to provide services or receive services in Fresno County is primary.

What are the key questions we want the Community Information Exchange to answer?

- Infrastructure – Real time data exchange
- Need to show "what you get" for the investment in real-time.
- Need to be able to support those who are not yet ready to provide real time data
- Understanding what level of support does an individual need in Fresno County to be successful?

What are the fundamental risks to the success of the Community Information Exchange?

- Lack of understanding regarding the use of the data, legal limitations regarding data sharing, bureaucracy, lack of organizational support to finish the project, funding.
- Alignment across different technologies, ongoing commitment to coordinating care, and governance bodies.

How will the Community Information Exchange engage partners to achieve success?

- Conversations and meetings to begin but also through targeted work with relevant participants. For example, working with the Health Department and a school district on a data sharing process based on needs.

Appendix E: Fresno CIE FAQ

What is the Fresno Community Information Exchange (CIE)?

The Fresno County Community Information Exchange (CIE) is an ambitious initiative aimed at transforming the way data is used to improve the lives of Fresno County residents. It focuses on creating an interconnected and data-driven community by enhancing data sharing technologies and cross-sector utilization for better care coordination and overall community well-being. This transformation is not just about improving service delivery; it's about fostering a collaborative environment where data can be used to address complex social and health challenges effectively.

Why do we need a CIE in Fresno County?

A real-time CIE will enhance the quality of life by addressing social determinants of health, providing comprehensive support to individuals, and ensuring timely access to resources and services. This interconnected system will improve prevention and response efforts, allowing us to understand and address both urgent and long-term community needs more effectively. By fostering collaboration and data-driven decision-making, the CIE will significantly enhance the overall well-being of Fresno County residents.

What are the main goals of the CIE?

- **Improving Care Coordination**: Streamlining case management and access to client information.
- **Reducing Duplication of Services**: Minimizing redundant data entry across different systems.
- **Enhancing Reporting and Data Access**: Providing real-time insights and comprehensive data analysis.
- **Suicide Prevention**: Integrating data from key agencies to offer timely support and resources to individuals at risk.

What are the two CIE pilots?

Within the CIE initiative, there are two upcoming pilot programs scheduled for 2024 that are set to make a significant positive impact in the community:

- **Suicide Prevention**: Fresno County recognizes the severity of the suicide crisis, with approximately 800,000 lives lost nationally every year. The CIE is proactively addressing this issue by integrating data from key agencies to provide timely support and resources to individuals at risk. This initiative marks a crucial step towards comprehensive multi-agency mental health care and suicide prevention efforts.

- **Home Visitation Services**: Fresno County is revolutionizing its home visitation services, which were previously hindered by inefficient data allocation. The CIE's cross-sector child and family data access pilot aims to streamline these services, resulting in improved outcomes for families, including increased kindergarten readiness, better maternal mental health, decreased trauma, and more effective service delivery.

What technological functionalities will the CIE offer?

- **Unified Integration Platform**: Central platform integrating data across all relevant systems and partners.
- **Advanced Data Analytics**: Real-time insights and comprehensive data analysis capabilities.
- **Alert System for Critical Health Indicators**: Automated alerts will support an immediate response by multiple agencies in times of great need.
- **Streamlined Workflow Management**: Optimized workflows, reducing redundancy and enhancing efficiency.

- **Enhanced Support System**: Centralized and comprehensive tool for managing billing, eligibility, and coordination of care.

What is the phased implementation plan for the CIE?

The CIE has a carefully structured plan for gradually integrating new technologies into existing workflows. This phased approach ensures minimal disruption and maximizes user adoption.

Which organizations are involved in the CIE?

- **CIE Core Team**: Fresno County, Fresno County Superintendent of Schools, Cradle-to-Career Fresno County.
- **Youth Suicide Prevention Workgroup**: Fresno County Department of Behavioral Health, Central Unified School District, Sanger Unified School District.
- **Home Visitation Workgroup**: Fresno County Department of Public Health, Fresno County Department of Social Services, Fresno Home Visitation Network.

What are the expected benefits of the CIE?

- **Improved Care Coordination**: Better management of client information and reduced duplication of services.
- **Enhanced Data Access and Reporting**: Real-time data insights and comprehensive analysis for better decision-making.
- **Streamlined Services**: More efficient workflows and optimized resource allocation.
- **Better Health Outcomes**: Improved maternal mental health, increased kindergarten readiness, and decreased trauma.

How does the CIE ensure data quality and compliance?

- **Centralized Data Management System**: Integrated case management and data sharing protocols.
- **Enhanced Data Quality Control**: Standardized documentation and outcome tracking.
- **Legal and Regulatory Compliance**: Adherence to all relevant laws and regulations for data handling and sharing.

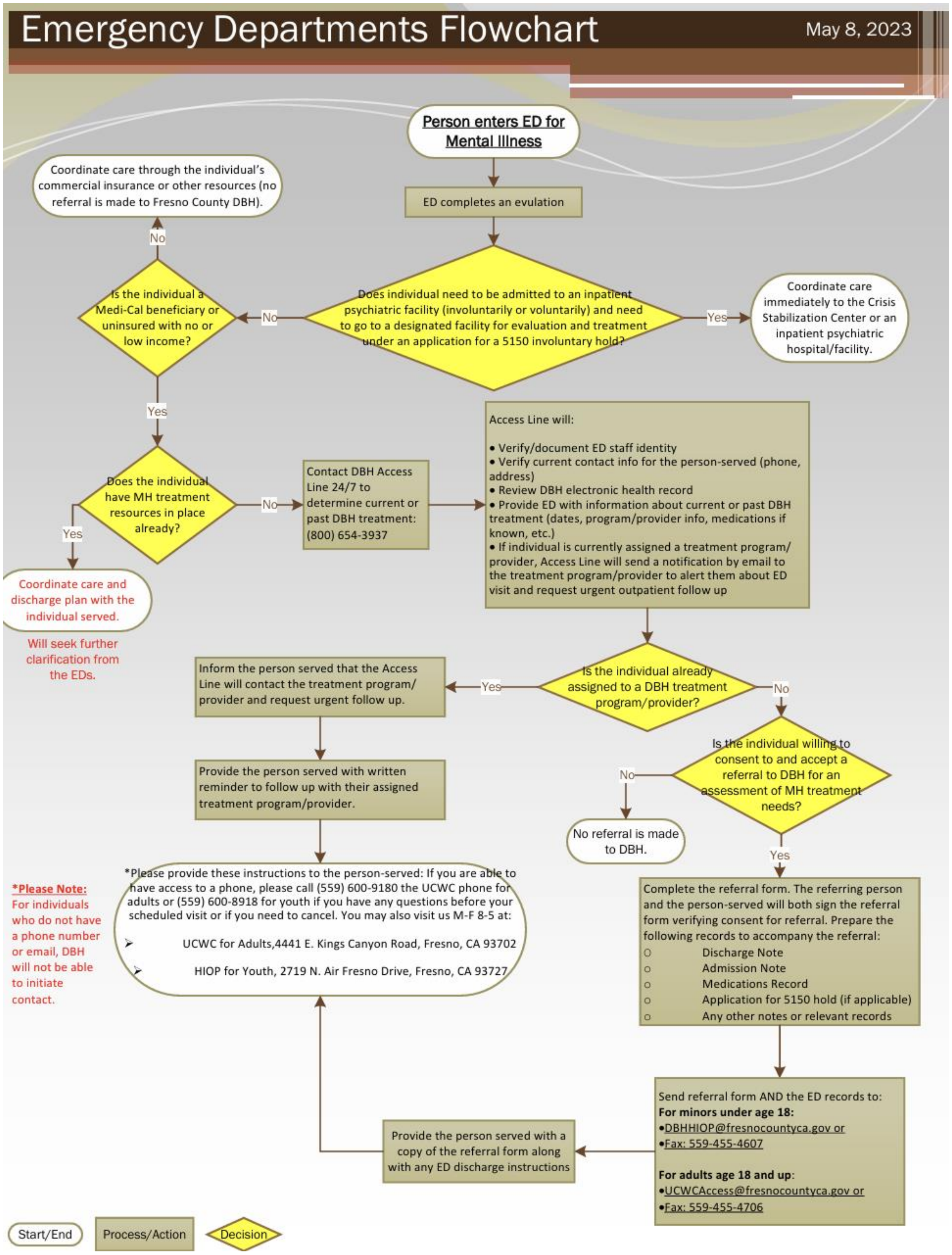
Who can benefit from the CIE?

- **Service Providers**: Better access to health and social service records for cross-care coordination between multiple sectors. Improved tools for managing billing, eligibility, and coordination of care.
- **Families and Children**: More effective service delivery and improved health outcomes.
- **Community Organizations**: Streamlined workflows and enhanced data sharing for better resource allocation.
- **Community Leadership**: Access to comprehensive data and insights to inform decision-making and policy development, enhancing community-wide health and well-being.

Appendix F: Fresno Example Narratives

Content under development by Fresno County team members and partners.

Appendix G: Current State Flowchart for ED 5150 Holds



Emergency Departments Flowchart

May 8, 2023

Person enters ED for Mental Illness

ED completes an evulation

Does individual need to be admitted to an inpatient psychiatric facility (involuntarily or voluntarily) and need to go to a designated facility for evaluation and treatment under an application for a 5150 involuntary hold?

Yes

Coordinate care immediately to the Crisis Stabilization Center or an inpatient psychiatric hospital/facility.

No

Is the individual a Medi-Cal beneficiary or uninsured with no or low income?

No

Coordinate care through the individual's commercial insurance or other resources (no referral is made to Fresno County DBH).

Yes

Does the individual have MH treatment resources in place already?

Yes

Coordinate care and discharge plan with the individual served.

Will seek further clarification from the EDs.

No

Contact DBH Access Line 24/7 to determine current or past DBH treatment: (800) 654-3937

Access Line will:

- Verify/document ED staff identity
- Verify current contact info for the person-served (phone, address)
- Review DBH electronic health record
- Provide ED with information about current or past DBH treatment (dates, program/provider info, medications if known, etc.)
- If individual is currently assigned a treatment program/provider, Access Line will send a notification by email to the treatment program/provider to alert them about ED visit and request urgent outpatient follow up

Is the individual already assigned to a DBH treatment program/provider?

Yes

Inform the person served that the Access Line will contact the treatment program/provider and request urgent follow up.

Provide the person served with written reminder to follow up with their assigned treatment program/provider.

*Please provide these instructions to the person-served: If you are able to have access to a phone, please call (559) 600-9180 the UCWC phone for adults or (559) 600-8918 for youth if you have any questions before your scheduled visit or if you need to cancel. You may also visit us M-F 8-5 at:

- UCWC for Adults,4441 E. Kings Canyon Road, Fresno, CA 93702
- HIOP for Youth, 2719 N. Air Fresno Drive, Fresno, CA 93727

No

Is the individual willing to consent to and accept a referral to DBH for an assessment of MH treatment needs?

No

No referral is made to DBH.

Yes

Complete the referral form. The referring person and the person-served will both sign the referral form verifying consent for referral. Prepare the following records to accompany the referral:

- ○ Discharge Note
- ○ Admission Note
- ○ Medications Record
- ○ Application for 5150 hold (if applicable)
- ○ Any other notes or relevant records

Send referral form AND the ED records to:

For minors under age 18:

•DBHHIOP@fresnocountyca.gov or

•Fax: 559-455-4607

For adults age 18 and up:

•UCWCAccess@fresnocountyca.gov or

•Fax: 559-455-4706

Provide the person served with a copy of the referral form along with any ED discharge instructions

Please Note: For individuals who do not have a phone number or email, DBH will not be able to initiate contact.