

Integrated human services data: Improving service provision for the super- utilizer population

*Population Health 780:
Public Health Principles and Practice*

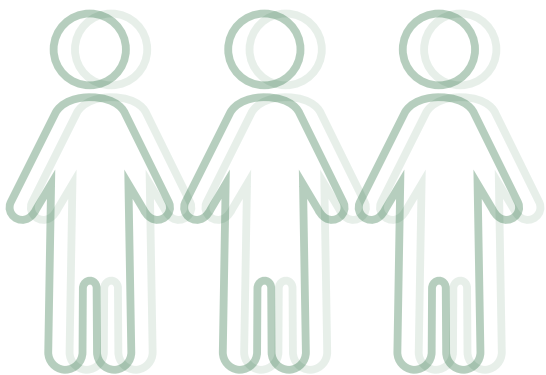


Table of Contents

Acknowledgements.....	iii
UniverCity Year – University of Wisconsin.....	1
Super-Utilizers and Integrated Data Systems	1
Benefits of Completed IDS Projects	3
Barriers.....	5
Funding	5
Initial funding.....	6
Maintenance Funding.....	6
Technical Barriers	7
System Structure	7
Unique Identifiers	9
Security	10
Organizational Culture as a Barrier to IDS Implementation	11
Political and Bureaucratic Power Relations.....	12
Bureaucratic Power Relations: The Interorganizational Context	12
Political Power Relations: The Policy and Social Context.....	13
Legal Barriers.....	14
Health Insurance Portability and Accountability Act of 1996 (HIPPA).....	15
Family Education Rights and Privacy Act of 1974 (FERPA)	15
Other Legislative and Regulatory Considerations	16
Key Considerations in IDS Implementation	17
Data Sharing Agreements and Memoranda of Understanding	17
Ethics of Aggregated Data	17
Recommendations	18
Conclusion	21
Appendix A: Information Integration Framework.....	22
Appendix B: Legal Resources	24
Appendix C: Sample Data Sharing Agreements.....	25
Appendix D: DCDHS Database Communication Structure	33
External Applications.....	33
Internal Applications.....	35
Appendix E: Recommended Readings	36
References	38

Acknowledgements

We would like to thank the Dane County Department of Human Services staff - Bill Hanna, Ron Chance, Lori Bastean and Jon Hatley – and Lila Walsh, in the Dane County clerk’s office, for their time, expertise and guidance.

We are thankful to the various state of Wisconsin employees for their insights into integrated data.

Without the cooperation and support of the Dane County Board of Supervisors and the UniverCity project staff, we would never have had the opportunity to work on this project.

Special thanks to Professor Barbara Duerst for all her guidance and support throughout this project. We appreciated all your efforts and extra time spend editing our paper.

UniverCity Year – University of Wisconsin

Beginning in the 2016-2017 academic year, the University of Wisconsin-Madison began the UniverCity Year program, a year-long partnership with a community in the Madison area. This partnership brings cross-disciplinary teams from UW-Madison courses to work on community-initiated projects.¹ For the 2017-2018 academic year, the university has partnered with the Dane County government. This project is the result of a collaboration between the UW-Madison School of Medicine and Public Health (SMPH) and the Dane County Department of Human Services (DCDHS).

DCDHS and the Dane County Board of Supervisors have identified “super-utilizers” of human services as a population who would be more effectively served by a coordinated response. The super-utilizer population’s needs, while possibly being met individually and in isolation, would be better met through coordination. In an effort to meet this goal, DCDHS has asked *Public Health: Principles and Practice* Master of Public Health (MPH) students at the SMPH to look at the benefits and barriers of data integration as it relates to the super-utilizer population.

This report is intended to be an initial overview of challenges and benefits represented in the larger literature. It provides a foundation for future work. Ultimately, internal staff will need to modify these findings using their Dane County specific expertise.

Super-Utilizers and Integrated Data Systems

The concept of a super-utilizer of services is one of increasing interest in the governmental, social, and services sector. The phenomenon was first described in the medical field examining patterns of use in emergency rooms.² The idea has since filtered into the human services field. As the use of this concept has expanded, so has the terminology. There are many synonymous terms used in the literature, including *super-user*, *high utilizer*, *frequent utilizer*, and *high-cost user* with super-utilizer being used commonly.

There are two different types of definitions for super-utilizers: general and operational. General definitions are much broader, are geared toward a lay audience, and typically include descriptive characteristics of the super-utilizer population. Specific or operational definitions are used for analysis and typically use counts, distributional cutoffs, or other types of thresholds to determine inclusion and exclusion in the sample. A few examples from the literature are provided below:

- 4 jail and 4 shelter admissions in last 5 years (count)³
- Risk score in top 20% of expected future cost (distributional cutoff)⁴
- Serious mental health diagnosis AND two or more hospitalizations in a 12 month period (condition-based threshold)⁵

Because operational definitions require thorough examination of the data to determine appropriate thresholds for inclusion, this type of definition will ideally be determined by DCDHS staff upon completion of the data integration project. This report uses a general definition based on the existing literature, which is provided below.

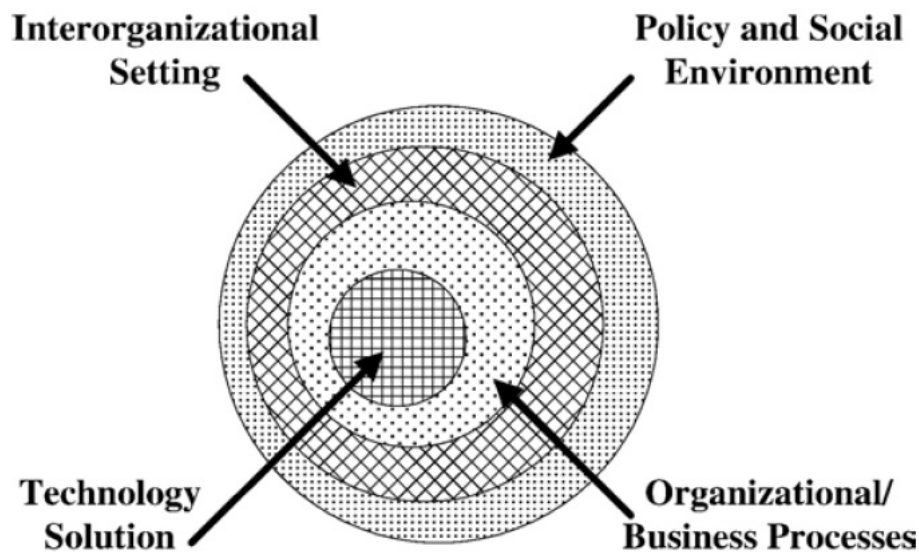
Super-Utilizers are individuals with complex behavioral, physical, and/or social needs, who are frequent and high-cost users of a broad range of criminal justice and social services, and would be more effectively served through a coordinated response.

The challenges super-utilizers face are compounded by systemic failures to meet the population's needs. Addressing the complexity of super-utilizer cases requires human services organizations to provide a variety of services across medical and social systems.⁴ However, these different systems often fail to communicate, resulting in divided, incomplete, and redundant service delivery.⁶ In San Diego, analysis uncovered that \$1.5 million worth of medically-related costs were being spent on 15 homeless individuals in the county.⁷ Investigations in different geographic areas find similar spending patterns with as little as 5% of a population consuming 49% of health related costs.⁸ The super-utilizer population's problems are a community-wide issue because individuals are not receiving services they require and communities are paying a staggeringly high price.

To address this problem, some state and local/municipal governments around the U.S. have attempted to consolidate their administrative and programmatic data in order to better serve their constituents. These Integrated Data Systems (IDS) can increase program effectiveness, improve services, and reduce operational costs by providing benefits in a range of micro- and macro-level settings.^{9,10}

To better contextualize the benefits and barriers of IDS in the public sector, this report draws on Pardo and Tayi's information integration framework.¹¹ This framework acknowledges that IDS technologies are embedded within four distinct contexts – Technical, Organizational, Interorganizational, and Political/Social – each with its own theoretical and professional perspectives (Figure 1 and Appendix A). A key advantage to this framework is that it does not separate social functions (individuals, organizations, and policies) from technical functions (IDS). Rather, it recognizes that social and technical functions need to complement each other in order to achieve the best results. This framework was the guiding structure for this paper. It is implicitly referenced throughout the various sections. A more formal discussion of Pardo and Tayi's framework can be found in Appendix A.

Figure 1: Nested Contexts of IDS



Source: Pardo and Tayi (2007)

IDS program planners at DCDHS will want to thoroughly examine the various benefits and barriers of the project and determine how the project fits within these different contexts.

The following section discusses the various benefits organizations can expect following the completion of an IDS project. The remainder of the report will detail commonly cited barriers to IDS implementation and methods to address them, discuss the key considerations of data sharing agreements and the ethics of integrated data, and will conclude with a description of suggested next steps for DCDHS and the Dane County Board of Supervisors.

Benefits of Completed IDS Projects

Developing and implementing an IDS is a serious undertaking. This investment requires serious consideration of the benefits and costs of such a system. The following is a discussion of the many benefits of a successful IDS system.

Cost Savings

IDS can be a costly investment. However, it is ultimately cost saving. For example, Michigan has integrated many of their departments at a state level into a system called BRIMM. They estimate that they have saved \$200 million annually since 2005 or \$800 million total. Of that, \$97 million was due to fraud recoveries. They credit improved administration of healthcare services, ability to conduct advanced analysis, ability to perform superior program assessment, detection of waste and fraud, and streamlining operations as the reasons for their cost savings.¹² Utah also mentions that their system reduces costs. The external verification of eligibility using data sources like eFind and the Department of Workforce Services' allows a more automated, verifiable process. It decreases the need to rely on self-reported client data and offers fewer chances for staff to make manual transcription errors. Moreover, more timely updates, through an IDS, on changes in circumstances that affect benefit levels can reduce the need to recoup payments later.¹³

Improved outcomes

IDS are necessary to accurately identify super-utilizer populations across service providers, and subsequently design, manage, and evaluate public intervention programs leading to improved outcomes. In Michigan, they have been able to successfully reduce childhood lead poisoning by 35% using BRIMM. Through analysis, government officials identified 14 communities that represented roughly 80% of all childhood lead poisoning cases. This has allowed the state to target their interventions to these communities specifically, something they would not have been able to do without an IDS.¹²

Moreover, because interorganizational cooperation is required to form and maintain a successful IDS, this allows for reinforcement of government-wide policy goals, which leads to more cohesive interventions for large problems such as inequality, education, nutrition, and poverty.¹⁰

Additionally, IDS can lead to more cost-effective research and community needs assessments. Organizations can use administrative program information to obtain large samples at lower costs than would be the case with surveys. It also helps to avoid underreporting and selection biases known to be associated with survey responses about program participation.¹³

Increased efficiency

IDS has the potential to increase efficiency at multiple levels. IDS can reduce duplicate data collection and storage within and between organizations, thereby decreasing the maintenance costs associated with all public programs.¹⁰ This shared data can then prepopulate forms and reduce need for clients to provide the same information and documentation to multiple agencies. This reduces the burden on staff. For example, in Utah, the process of checking other data sources to verify eligibility information was reduced from 17 minutes to 3 minutes after the implementation of their IDS. Additionally, according to a report by Michigan's Department of Technology, Management, and Budget, since the use of BRIMM, individual case benefit redeterminations are 50% faster.¹³ This efficiency not only impacts system users, but also program administrators. A well implemented IDS allows program administrators to access accurate data in a timely manner, a crucial component in effective decision-making.⁹

Ease of use for clients

The integration of data can significantly reduce the burden on clients since client data is shared and does not have to be repeatedly collected. Clients do not always have the needed documentation with them, nor are they always able to clearly describe their history or situation. Utah reduced the amount of documentation a client must submit. For example, clients may not have to submit pay stubs if eFind has timely wage and employment information. This makes the eligibility verification process more uniform and user friendly. Auto-population of data is particularly important when dealing with clients who are unable to reliably relay information. For example, in New York, their IDS has allowed them to better serve a transient population with a high burden of behavioral health and insecure housing situations. IDS can decrease eligibility turnaround time for clients and help caseworkers contact families if limited or inaccurate information was provided on intake, as is the

case in Alleghany County. Michigan has taken this one step further and now, with the use of BRIMM, has one caseworker across programs for each client.¹³

Improved organizational capacity

IDS can provide a wide range of benefits within the organizational context. IDS can help in the formation of standardized definitions and data collection processes. This standardization can mitigate institutional knowledge loss and facilitate further knowledge and data sharing (both intra- and inter-organizational). IDS can also improve organizational and programmatic decision-making processes and increase coordination within an organization.¹⁰ Lastly, IDS and other coordination tools can build and strengthen professional networks, which in turn support successful collaboration and innovation within an organization.^{10,14,15}

Improved accountability and public perception

Timely access to accurate administrative data promotes accountability, which helps align organizational practice with broader societal and public values.^{10,16} Increased productivity, effectiveness, and innovation can strengthen an organization's reputation among the general public and their perceived value among policymakers.^{10,17}

Increased interorganizational collaboration

IDS both requires and facilitates interorganizational cooperation. The process of creating an IDS leads to strengthened professional networks, a sense of shared ownership and sustained collaboration.^{15,18} IDS can help participating organizations understand how they are operating as a collective, allowing them to more efficiently allocate resources, effectively target at-risk subpopulations of users, and integrate long-term strategic planning.^{9,10} This results in improved productivity, service delivery, and cost-effectiveness.¹³

Barriers

While there are many benefits from IDS, implementing one can be time consuming and challenging. Below are the most commonly cited barriers, real and perceived, with examples of how to successfully overcome them.

Funding

Creating an integrated data system is a long-term, large-scale, and resource intensive project. Alongside a multitude of other decisions and plans that need to be made, securing short-term and long-term funding is a priority. In a survey of eight completed IDS projects considered to be exemplary,⁹ initial funding for infrastructure ranged from \$50,000 to \$800,000 with an outlier project spending far more. Additionally, four of the eight systems surveyed had a specified and ongoing maintenance budget.

Initial funding

Issues to Consider

Funding the initial phases of an integrated data system during the creation and implementation is a challenge. First, an integrated data initiative requires a large amount of expensive and specialized resources dedicated to the project. Depending on the system structure, the project will require public services employees to help design the system, developers to code the system, hardware to store and/or access the data, and time for end user training.¹⁹ Second, federal funding for technology related initiatives can be attached to complicated specifications about how the money can be used and for which specific programs. When the technology project strives to create one integrated system, rather than program specific systems, administrators can run into issues with reimbursement. Third, even when funding is available, legislators might be hesitant to allocate all the necessary funding upfront fearing that the project might not be successful.²⁰

How to Address Issues

Although securing initial funding is challenging, counties with integrated data systems have successfully navigated the three main barriers mentioned in the previous section. Across many integrated data system initiatives, initial costs remained high. However, Allegheny County found a promising funding route to avoid the issues with federal regulations and reimbursements by utilizing the Human Services Integration Fund (HSIF).²¹ The fund is sustained by a growing group of local, private foundations that share the desire to improve the quality of public services through supporting projects such as those relating to public service technology innovation. Some examples of participating organizations are the United Way of Allegheny County, The Pittsburgh Foundation, and the Richard King Mellon Foundation.²¹ The HSIF financially supported Allegheny County's integrated data system project as part of a larger Department of Human Services restructuring project that the HSIF was contributing to. Having the philanthropic support of local groups in southwestern Pennsylvania was crucial to Allegheny County's success because it allowed them financial flexibility that would have been very difficult to achieve with public funding.²⁰

If seeking private funding is not the optimal solution, Idaho provides an example of how to work with legislators to secure government funding. The Idaho legislature supported the Department of Health and Welfare's technology project, while remaining cautious. Legislators agreed to the total amount of funding needed, but released the funds on a gradual basis as verifiable progress benchmarks were met.²⁰ The gradual payments made it possible for the project to balance both the Department of Health and Welfare's and state legislators' needs.

Maintenance Funding

Issues to Consider

Once an integrated data system is established and incorporated, resources must be dedicated to maintain the system. The system might require periodic hardware upgrades, security reviews and updates, data management, and system improvements that will need the attention of staff to complete. Based on a survey of both county and state integrated data systems, the average number of full time staff needed to maintain these systems was around three, however, these employees

typically only dedicated a maximum of quarter of their time to maintaining the system.⁹ Although day-to-day maintenance might not require the same volume of funding as the initial phase of the project, it is still a critical piece.

How to Address Issues

Allegheny County maintains their DHS Data Warehouse mainly through federal and state funding with occasional grants. Their IDS system makes staff more efficient resulting in net decreased spending for the county.¹⁸ Reports from the State of Michigan illustrate how an integrated data system can save a department money that can then be reinvested into maintaining the data system or elsewhere. By using their data warehouse to retrieve information rather than printing reports, the Michigan Department of Community Health (MDCH) saved the costs associated with printing and distributing these reports.¹² On a larger scale, the State of Michigan saw reductions in costs associated with duplicative and fraudulent services. MDCH workers were able to identify instances where an individual was receiving an identical or similar service from two different programs and correct the error. Likewise, MDCH workers could review an individual's program eligibility and prevent benefits from being sent to deceased individuals.²² MDCH quantifies the savings attributable to their integrated data system, when considering things like overall savings and avoided sanctions, to be around \$200 million annually on the state level.²³ Groups with integrated data systems are able to financially maintain their systems through small and large-scale budget changes.

Technical Barriers

An integrated data system must be designed to support the workflows of its end users by helping them make informed decisions about their clients' needs. The technical aspects discussed in this section are focused on the behind the scenes portion of the system, not what end users interact with, and deal with high-level system structure considerations. From reviewing the literature, there are three overarching technical considerations when creating an integrated data system: the system structure, how individuals in the system will be identified, and security.

System Structure

Integrated data systems for public services typically fall into two categories: repositories or portals. Repositories and data warehouses are systems that collect and centrally store information from multiple systems, making it easy to extract and review data in different formats. Portals differ from repositories in that information from multiple systems is not centrally stored anywhere, rather, users view data stored in multiple systems simultaneously through one interface. The following paragraphs explain the benefits and drawbacks of each system followed by case studies that exemplify best uses for each structure.

Issues to Consider: Repositories and Data Warehouses

Using a repository or data warehouse structure, rather than a portal, allows for easy control and maneuvering of the data, as data from a variety of systems undergoes an import and standardization process to fit into the central storage structure.¹³ The uniformly stored data is a huge advantage of the data warehouse structure because it makes it possible to easily query the system and extract

desired information without having to consider limitations that might be present due to how various systems may incompatibly store data. For example, before standardizing the data, date of birth may be stored differently in different systems such as DD/MM/YYYY in one system and MM/DD/YYYY in another. Standardizing the data from all systems to be stored in the data warehouse frontloads the effort needed to compare data across systems. The data structure makes it simple to automatically generate reports on an ongoing and predetermined basis and get necessary information without much manual effort.²² Aside from the benefits of standardized data storage, using a repository includes the option to store historic data even if the individual systems do not retain data at all or for as long as is needed.¹³ Additionally, creating a central repository or warehouse allows individual organizations to continue using their current, source systems with little or minimum disruption to daily workflows.²⁴ The majority of IDS that we reviewed are central repositories.

A system as robust and flexible as a repository or warehouse has two major drawbacks. First, data must be transferred from the source systems to the warehouse through an extensive exporting, importing, and cleaning process. Departments using a data warehouse structure report that this type of maintenance can consume the vast majority of technical resources.¹³ Second, there can be a delay between the information in the data warehouse, in the reports, in the source systems, and in reality. Data warehouses can be refreshed on a set schedule, such as monthly, weekly, or nightly, however, this makes it unlikely that the stored data can be used for decision-making in real time.¹³

How to Address Issues: Repositories and Data Warehouses

Some public service providers have had success using central repositories and data warehouses for their integrated data system needs. Two examples of this type are Michigan's Enterprise Data Warehouse and Allegheny County's Department of Human Services' Data Warehouse. Michigan's system was created in the 1990s with the initial purpose of reviewing Medicaid claims, but has since grown to include data from groups such as the Department of Human Services, Corrections, and Natural Resources, as well as sources like the police, court systems, and federal data sets.¹²

Users of the Michigan Enterprise Data Warehouse benefit from the centrally stored data because of the ease and flexibility it allows them in pulling different information simultaneously, despite the slight lag time that is a result of nightly refreshes. For example, when employees at Michigan's Office of Child Support are attempting to find a parent that has missed child support payments, they are able to leverage records outside of their department, such as hunting licenses, to get more information on the individual they are trying to find.¹³ In addition to being able to complete ad hoc searches, Michigan's staff benefit from automatic report generating capabilities. The system creates predetermined reports on a set schedule on topics such as Health Plan Key Indicators.²² Lastly, some of the data that is imported into the Enterprise Data Warehouse is stored long-term, such as what services individuals received, for comparison against current data.¹³

Allegheny County's DHS Data Warehouse came out of the department's restructuring in the early 2000s, during which they took the opportunity to review the documentation tools they were using for behavioral health and homelessness related data. The system has since grown to include data from departments within and outside DHS, such as Pittsburgh Public Schools, corrections facilities, county and city housing authorities, and public welfare programs²⁵ with the goal to

continue adding data from additional sources such as hospitals and clinics.²⁶ The ease of pulling data from vastly different systems through the data warehouse is crucial for workers to get an adequate understanding of their clients. For example, with the integration of public school data, DHS workers can review a child's attendance at school and consider it in relation to recent changes at home.²⁴ In addition to the aggregated client-level data, the data warehouse enables Allegheny County to examine their aggregate/composite de-identified data, so as to understand the larger trends of the communities they serve. One example of how Allegheny County benefits from their data warehouse is that they were able to utilize their data to identify that, over the course of one year, the number of children on welfare that also accessed mental health services increased by 18 percent.²⁴ The Allegheny County DHS Data Warehouse has helped the county serve their population's individual and collective needs.

Issues to Consider: Portals

Portal systems are used in similar ways as data warehouses, but the storage structure gives portal systems slightly different advantages and disadvantages. Like repositories, portals can be used to find aggregated data about an individual from multiple sources. However, the data remains stored in multiple different systems owned by different organizations. By using a portal instead of a data warehouse, an organization does not need to supply the resources for standardizing and storing data in the same way as would be needed for a data warehouse.¹³ An additional benefit of using a portal is that client information can be found in real-time, making the public service providers ability to assist the client easier and faster.²⁷

Although the portal structure enables employees to view comprehensive data about a client, it does not have the same flexibility as a data warehouse. Since the data is not standardized in order to be centrally stored, the data maintains all the limitations of the source systems such as how the data is stored and how long it is kept.²⁸

How to Address Issues: Portals

New York City's Worker Connect system is an example of a successful portal system. In the early 2000s, interoperability between human service organizations was a pressing need. The data sharing project had the goal of making it easier for public service providers to access a variety of information about a client. With the creation of Worker Connect, employees can view comprehensive client information by logging into just one system.²⁹ One example of how Worker Connect successfully helps public service providers is in the case of a homeless individual seeking shelter. An individual might arrive without the necessary paperwork. With the portal, an employee can pull their demographic information, previous experiences in shelters, and other data from the system to process the individual. Having access to multiple data systems saves time for the employee and allows clients to receive the services they need on an expedited timeline.¹³

Unique Identifiers

Regardless of the structure, the system will need to have a method of linking records together that are associated with the same individual. Finding related records can be technically challenging and is further complicated by the challenges that super-utilizers face. The following section presents the challenges in identifying records and examples of how these challenges can be overcome depending on the system structure.

Issues to Consider

Super-utilizers that repeatedly and frequently interact with public services are likely to be managing one or more medical, substance, or social issues.⁴ This array of issues could make it challenging for an individual to be willing or able to give accurate identifying information at every interaction with a public service institution. For example, clients sometimes give alternate name spellings or inaccurate date of birth information for a variety of reasons.²⁶ Social Security numbers are sometimes used to match client records across systems, however, disseminating even part of a Social Security number can enable identity thieves.¹³ Since matching client records will be a challenge, the integrated system must be designed to address it.

How to Address Issues

The most comprehensive way to link records that relate to the same individual, and the way that most systems address this issue, is through an automated process that compares the records on multiple levels, such as name, date of birth, and addresses and then links the records only when a sufficient amount of data matches.²⁶ Once the records are determined to sufficiently match, Michigan's Enterprise Data Warehouse¹² and Allegheny County's DHS Data Warehouse²⁵ assign client identifiers to every record that corresponds to that individual in order to facilitate searching for and aggregating that data at a later time. New York's Worker Connect portal also evaluates demographic data to create a match. However, since the Worker Connect system is a portal and cannot centrally store data like the previously mentioned systems, rather than assigning and saving an identifier, the system maintains an index of that client's information in various systems in order to be able to find comprehensive information about an individual when needed.²⁷

Security

Along with the ease of access to a breadth of client data comes the risk of data being used inappropriately. Maintaining security from internal and external threats is an integral part of designing and maintaining a functional system. This section examines a selection of security threats and offers examples of protective measures.

Issues to Consider

Data security could be threatened internally when employees have access to more information than is necessary to complete their tasks, or employees access information outside of work related task.¹³ Externally, data that is being stored or transmitted is vulnerable to hacking which could result in data being undesirably used or exposed.³⁰ Additionally, it is important to have a de-identification process in place so that sensitive information is not needlessly disclosed.²⁶

How to Address Issues

Organizations typically have multiple layers of security to be sure that the data is safe from internal and external threats. To address the internal threats of employees accessing information that is not necessary to their daily tasks, Worker Connect, Michigan's Enterprise Data Warehouse, and Allegheny County's Data Warehouse require employees to use passwords to access the system and limits the information an individual is able to see based on their role. Additionally, users are trained on appropriate uses of the systems and are informed of the extensive auditing capabilities that will record who accesses what information and at what time.¹³ Informing users about the importance of auditing and how it will be used helps build a work culture that is attentive to the

security needs of an integrated data system. To address the external threats from hackers, human and hardware resources should be dedicated to designing and maintaining a system that adheres to security best practices put forward by organizations such as the International Organization of Standards.³⁰

Lastly, since the data will be used to compare characteristics of clients in different organizations, the system needs to have a process for removing identifying information while maintaining the usefulness of the data. Allegheny County's DHS Data Warehouse has a four-step process to de-identifying their records that includes removing names and numerical identifiers, inserting age instead of date of birth, and removing geographic descriptors.²⁶ De-identifying the data makes it possible to examine large trends without compromising the security of confidential client information.

Organizational Culture as a Barrier to IDS Implementation

The beliefs, motivations, values, and norms of both individuals and an organization, in other words, organizational culture,³¹ have the potential to aid in the successful implementation of a project or derail it before it can begin. In a Government Accountability Office (GAO) report to congress, stakeholders identified anti-data sharing mindsets, lack of trust in other agencies, and insufficient training opportunities as “extreme” or “great” challenges to IDS implementation.¹³ Additionally, in a systematic review of 65 separate articles discussing barriers to data sharing in public health by *van Panhuis et al.*, 30% of all barrier types related in some way to personal and organizational beliefs, motivations, or misconceptions.¹⁹

Issues to Consider

IDS implementation barriers relating to culture are particularly difficult for organizations to overcome. First, these barriers are often highly inter-related. For example, insufficient training opportunities may lead to an overall lack of confidence in areas requiring technical expertise. This in turn may lead to a general anti-data sentiment. This, in turn, could increase organizational resistance to data usage, cultivating a lack of trust in agencies that *do* use data, and so on and so forth. Second, organizational culture constitutes the deepest, most stable, and least malleable characteristics of a group.³¹ This can make IDS implementation extremely difficult in organizations with strong anti-data sharing cultures, especially if those organizations have long histories or particularly negative experiences with data and IDS.

How to Address Issues

Without intimate knowledge of the organization, it is difficult to provide DCDHS with specific methods for overcoming cultural challenges as they relate to IDS. However, there are broad cultural characteristics that may promote and encourage successful data sharing projects. First and foremost, organization-wide buy-in is paramount for successful IDS implementation. For some organizations, achieving buy-in may only require a funding source and the conversion of a few key holdout employees. For other organizations, more drastic, transformative changes may need to take place to ensure all employees are on the same page. In both cases, strong leadership is needed to effectively communicate the overall vision of the project as well as expected benefits for individual stakeholders.^{10,31} There are also specific organizational characteristics that have

been shown to have positive correlations with successful implementation of new technology systems. These include, but are not limited to, sharing information freely, working closely with others, team oriented work, and trust.³²

Washington State's Research and Data Analysis Division's experience developing their Integrated Client Data Base (ICDB) provides a concrete example of how to overcome organizational culture barriers. In the words of Rebecca Yette, a project leader, "[I] didn't realize how many barriers there would be and how resistant people would be, or that people would just think it wasn't possible and they didn't want their staff to spend time even dealing with it."³³ However, project leaders believe their optimism ultimately helped push the project through to completion. Additionally, project leaders fostered trusting relationships between researchers and practitioners, which created buy-in, a sense of entrepreneurialism, and a free flow of information within the organization.

Political and Bureaucratic Power Relations

Political and bureaucratic power relations can be major barriers to IDS implementation. These barriers primarily take place within the interorganizational and policy/social contexts, and center around questions of data ownership and governance. As one State of Wisconsin contractor stated, "data ownership is always political, even if you don't want it to be."

Bureaucratic Power Relations: The Interorganizational Context

Issues to Consider

Within the interorganizational context, there are a number of factors that contribute to political and bureaucratic barriers. First, as the public sector has increasingly collected and analyzed administrative and programmatic data, ownership of this content has become a source of both pride and power for government organizations. As program efficiency and effectiveness have become top priorities for policymakers, data and the ability to analyze it have become primary contributors to agency reputation.³⁴ In general, bureaucratic agencies seek to maximize their reputation and perceived value to policymakers in order to ensure continued funding.^{17,34} In extreme cases, large organizations that collect vast amounts of data may attempt to hoard that data and leverage their existing capabilities for increased appropriations. This allows them to amass more analytic and data collection capacity and in turn become more powerful. In the current political environment, where budget shortfalls and appropriation decreases are expected, government organizations may be hesitant to freely share resources (i.e. data) that bring them power, reputation, and enhanced public image.^{17,34}

A second and related factor contributing to bureaucratic barriers is the concept of data as an asset, rather than data as power. Organizations, both private and public, likely realize that the data they collect has value outside the organization. Rather than refusing to share data outright, organizations may be waiting for an opportunity with benefits that outweigh opportunity costs.¹⁹ In this scenario, agencies use their own data as a bargaining chip to increase overall data assets and analytic capabilities.³⁴

A third factor contributing to bureaucratic barriers, again, relates closely to agency reputation. Some organizations collect data but do not have the capacity to effectively analyze it. Others have the ability to analyze data, but not collect it. Collecting data is hard and expensive work, yet individuals and organizations who specialize in analysis typically receive most of, if not all of, the credit for improvement and innovation. Because of this, organizations that fall into the former category may be hesitant to enter into data sharing agreements.¹⁹

The final factor contributing to bureaucratic barriers is cost sharing, a topic that is discussed in the *Funding Barriers* section of this report (page 5). Most government agencies are experiencing budget cuts and will only share data when it is beneficial to them. As such, it is unlikely that these agencies will enter into agreements when up-front and maintenance costs are not distributed equitably.

How to Address Issues

A broader solution to interorganizational barriers is to attempt to reframe the ‘state of play’. This involves moving away from a framework of competition over scarce resources to one of collaborative innovation and problem solving to the mutual benefit all stakeholders.

Any attempted data sharing agreement should be mutually beneficial for all parties involved. Ideally, organizations should see concrete and immediate benefits to an agreement. It is unlikely organizations will agree to data sharing agreements if benefits are delayed or uncertain.¹⁹

Cost sharing structures should be as simple as possible, and should be formulated as early as possible. Decreasing administrative burden and the cost of entry for outside organizations will increase the likelihood of successful completion of data sharing agreements.

Many of the interorganizational, bureaucratic barriers can be overcome through well-crafted data sharing agreements. Strong leadership and collaborative organizational cultures will also help to facilitate successful IDS implementation. This will be discussed further in the *Data Sharing Agreements* section on page 16 of the report.

Political Power Relations: The Policy and Social Context

Issues to Consider

In addition to bureaucratic power relations, political maneuvering, both positive and negative, is likely to occur during IDS planning and implementation. Administrators of organizations attempting to implement IDS may experience both interference and support from political elites. These political elites (legislators, city/county officials, business owners, etc.) may either interfere with or support the program in an effort to exert control over the bureaucracy or to advance policy agendas (both personal and party).^{35,36} Due to the wide range of competing interests and the asymmetrical nature of power, political barriers are often nearly impossible to fully overcome. Efforts to address political barriers should focus mitigating negative effects through bolstering support for the project and aligning interests where possible.

How to Address Issues

The most effective way to mitigate political barriers is to align the interests of all stakeholders involved. Ideally, the DCDHS IDS project goals, strategic plan, legal considerations, and data structures will all align with the interests of private, state, and federal organizations. However, it is much more feasible to successfully achieve alignment in one of these areas and build momentum from there. Aligning project interests between stakeholders is often thought of as a consensus building activity, where project and organizational leaders develop a plan of action that suits all parties involved. While this is true, the overarching policy structure and methods of service provision within which these organizations operate also play a significant role in the ability of organizations to align their interests. North Carolina's Public Health Law³⁷ is one example of how policy structure can positively influence the likelihood of aligning multiple interests.

North Carolina's Public Health Law was passed in 2012, and allowed counties to try new approaches for organizing and governing local human services agencies. The law allows counties to create consolidated human services agencies (CHSAs), which provide all health and social services for the region. This service provision model provides an opportunity to coordinate services, eliminate duplicated efforts, and align the interests of the different divisions within the organization.³⁸ In contrast, the structure of human services provision in the state of Wisconsin is much more fragmented, making it more difficult to bring multiple parties to a consensus.

In cases where consensus building and aligning interests seem unlikely, organizations and their partners may need to seek allies in order to overcome political resistance. In these cases, executive sponsorship is one of the most important assets a project can have. Executives, whether that be a state governor, city mayor, or, in the case of DCDHS, a board of supervisors, have a huge amount of control over the political agenda.³⁵ If a project has executive sponsorship, it will be much easier to identify partners and negotiate advantageous policies and regulations. The second key group in bolstering project support is project champions. These are individuals who are highly supportive of the program and who work to convert those who are opposed to the project to become supporters.

These two points are reinforced by the experience of the project leaders of the Integrated Client Data Base (ICDB) mentioned in the previous section. In the mid-1990's, the secretary of Washington State's Department of Social and Health Services actively encouraged other agencies to share their data with the ICDB project. Additionally, as the project gained momentum, "key leadership champions emerged," which helped ensure the project's success.³³

Outside these two major ally types, organizations should simply seek to recruit as many allies as possible when facing political barriers. While not sufficient for success, a large and well-connected support base will be beneficial in overcoming political barriers and can help facilitate negotiations throughout the implementation process.

Legal Barriers

Legal barriers are among the most often cited reason for why an IDS is not feasible.¹³ In one GAO report, confusion or misperceptions around what agencies are or are not allowed to share was endorsed by 91% of the respondents.¹³ For example, in Alleghany County, many thought the

legal barriers would prove to be insurmountable prior to starting the project.¹⁸ Many providers cite privacy as a general concern but do not know the actual scope of the law. This often leads to agencies and agency lawyers being overly conservative and interpreting federal requirements more narrowly than required. There is also the challenge that most DHS providers are subject to multiple privacy requirements but do not always know which is applicable under which circumstance. Moreover, these rules are not well aligned and often contradict one another.¹³

There are many laws and regulations Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Family Education Rights and Privacy Act of 1974 (FERPA) are often considered the most important and potentially problematic when undertaking an IDS.

Health Insurance Portability and Accountability Act of 1996 (HIPPA)

Issues to Consider

HIPPA applies to the protection of individually identifiable health information and applies to health care providers, health plan and health care clearinghouses. Protected health information (PHI) may not be disclosed without authorization except for use in treatments, payment or health care operations.¹³

How to Address Issues

In order to use PHI, one can either get consent from the individual, which is often inconvenient and impractical in regards to IDS, or one can de-identify person level data records. While de-identification does not allow for person specific databases, in an IDS system, it allows one to get a better picture of service users and patterns. For example, in Alleghany County, this work around allowed them to get a better picture of mental health, drug treatment and CPS overlap. They had initially thought CPS was a major entry point into their social services but through their data analysis they realized mental health treatment was the biggest entry point for families. They also used census block data to geolocate users allowing them to locate services into high need areas.²⁶

To de-identify records:

- Strip out names
- Replace personal identifiers like SSI with arbitrary sequence number
- Replace date of birth with age
- Replace street address with census block²⁶

Family Education Rights and Privacy Act of 1974 (FERPA)

Issues to Consider

FERPA is a federal law that requires protection of personal educational information by all education agencies and institutions. Parents have the right to inspect their child's record and must give written consent to release information. Directory information including name, address, telephone, birth date/place, degrees, and dates of attendance may be given out without written consent though parents have the right to opt out.¹³

Of all the privacy laws, this law, in particular, is often singled out as too restrictive. For example, caseworkers are required by law to include school records in their plan for children in the foster care system, however schools cannot give caseworkers access to those records without parental permission or a court order.¹³

How to Address Issues

A 2008 FERPA amendment permitted release of personally identifiable student data without consent to organizations interested in conducting research to improve student achievement as long as these organizations signed a MOU that outlined confidentiality parameters and data use protocols.¹⁸

Other Legislative and Regulatory Considerations

There are many laws that have implications for an IDS and they vary greatly by locality. Table 1 is a list of important federal and state privacy laws. It should not be considered exhaustive. Additional resources around privacy laws and solutions to them is presented in Appendix B.

Program/Service Area	Governing Body	Act/Regulation	Legislative Code
General	Federal Federal	Privacy Act of 1974 Internal Revenue Service Regulations	IRS Section 6103
Education and Students	Federal State State	Family Educational Rights and Privacy Act (FERPA) Wisconsin Pupil Records Law Wisconsin Policy Regarding Pupil Identification Numbers	Wisconsin Statute §118.125 Wisconsin Statute §118.169
Health	Federal Federal Federal	Health Insurance Portability and Accountability Act (HIPAA) Health Information Technology for Economic and Clinical Health (HITECH) Patient Protection and Affordable Care Act	
Child Welfare	Federal Federal Federal Federal Federal Federal Federal	Statewide Automated Child Welfare Information Systems (SACWIS) Child Abuse Prevention and Treatment and Adoption Reform (CAPTA) Child and Family Services Improvement and Innovation Act Fostering Connections to Success and Increasing Adoptions Act Social Security Act: Title IV-E Social Security Act: Title IV-B Social Security Act: Title XX	
Supplemental Security Income for the Aged, Blind, and Disabled	Federal	Social Security Act: Title XVI	42 USC §1381
Supplemental Nutrition Assistance Program (SNAP)	Federal		7 USC §2011
Temporary Assistance for Needy Families (TANF)	Federal	Social Security Act: Title IV-A	42 USC §601
Child Support and Establishment of Paternity	Federal	Social Security Act: Title IV-D	42 USC §651
Violent Crime Control and Law Enforcement	Federal State	Violence Against Women Domestic Abuse Services	42 USC §13925 Wisconsin Statute §995.67
Mental Health/AODA	Federal Federal	Public Health Service Act Confidentiality of Alcohol and Drug Abuse Patient Records	42 CFR Part 2

Current distrust in government and privacy concerns have led to a breeding ground for myths, misinterpretations, and half-truths surrounding IDS privacy regulations. This makes the creation of legal agreements very important, but time consuming. Legal counsel is vitally important for this process. It is particularly helpful to have general counsel that understands the intricacies of the world of Big Data as they are experienced in MOU creation and the federation, state and local laws governing use of permissible use of data.

Key Considerations in IDS Implementation

All barriers mentioned in the previous section should be taken into account when planning and implementing an IDS project. However, there are two key components to IDS planning that are absolutely necessary to achieve success and span multiple barriers. The following section will discuss data sharing agreements or memoranda of understanding (MOUs), and the security, privacy, and ethics of aggregated data.

Data Sharing Agreements and Memoranda of Understanding

Data sharing agreements are the foundation of any IDS project. The best data sharing agreements will act as mechanisms to address or eliminate the technical, legal, organizational, and political barriers to IDS implementation above. They are one of the first components organizations must complete in an IDS project, and therefore have the potential to build momentum and streamline later steps in the implementation process.

Because data sharing agreements address multiple barriers, the characteristics of high quality data sharing agreements mirror the “potential solutions” outlined above. Namely, high-quality data sharing agreements will align the interests of the stakeholders involved, particularly those at higher levels of government (i.e. state or federal level). This increases the likelihood of additional successes in data sharing agreements with other lower-level organizations, because the framework will be approved by the larger governing entity and will be uniform from location to location. Additionally, data sharing agreements will address the ethical data usage issues that will be discussed below.

Examples of data sharing agreements are included in Appendix C.

Ethics of Aggregated Data

Aggregated data is a powerful tool for public service providers seeking to administer more coordinated and comprehensive support to super-utilizers. However, an integrated data project is something that must be pursued diligently and thoroughly as it brings the potential for data to be inappropriately revealed. Some key considerations for undertaking an aggregated data project are data governance and data stewardship.

Keeping sensitive information about an individual confidential is the basic and expected duty of an organization that aggregates data.³⁹ In order to have secure data practices, organizations need

to explore the concepts of data governance and data stewardship. Data governance refers to the underlying framework that guides data stewardship, which is the more practical implementation of keeping data secure through specific processes relating to things like data storage and sharing.⁴⁰ These concepts serve to reinforce the duties that organizations have and facilitate a clear understanding between them and the individuals whose data is stored. A main challenge to an organization becoming a good data steward is the limited national standards for aggregated public health data. Although the Model Public Health Privacy Act does put forward some key considerations for privacy and security, the implementation of these guidelines still requires organizations to engage in discussions about ethical data use.⁴¹

When organizations do embark on constructing ethical guidelines for data usage, there are a variety of key components that should be considered. First, organizations should establish guidelines that detail appropriate uses for data, such as if data will be used to assist individuals, used for large scale analysis, or both. Second, organizations need to reach decisions around sharing data, such as with what organizations are they permitted to exchange data with³⁹. In discussions about who data can be shared with, it is important to consider who is the ultimate owner of the data, is it the individual or the organization⁴⁰. And lastly, organizations need to be mindful about the culture surrounding big data and strategically move through it. Collecting sensitive information makes the tension between the benefits of big data and personal privacy especially salient⁴⁰. Over the course of history, there have been instances of surveillance data being used to reduce personal privacy and autonomy.³⁹ Although guidelines and expectations surround big data have shifted, society may have an instinctive distrust of large-scale data aggregation. Overall, when an organization initiates a data integration project they must consider both the high-level and detailed ethical implications.

Recommendations

Building an integrated data system that will meet Dane County's needs is possible by navigating the technical, financial, legal, and organizational barriers. In order to address these various needs, DCDHS should take a systematic approach to assessing needs, defining a plan, and then taking action. Based on discussion with DCDHS personnel, the department currently has the capability to examine cost per case for the majority of cases within the department. DCDHS also currently has the ability to match many cases with data from criminal justice services. Future actions should focus on reinforcing internal business rules and process flows, addressing gaps in data collection from subcontracted agencies, developing the legal framework that will facilitate future data sharing with external agencies, and discussing workarounds for data challenges arising from state IT systems. Addressing these issues will put Dane County in an excellent position to establish a county-wide integrated data system to better serve their clients.

Short Term (High Priority)

Create an interdisciplinary IDS project design team

Identify what staff members in DCDHS can be recruited to help with the technical, legal, and financial aspects of an integrated data system project. Staff from these three areas of expertise will need to work closely with one another to identify potential challenges, determine funding needs

and sources, develop high-quality data sharing agreements, and create an implementation and evaluation plan. Additionally, individuals with non-technical knowledge, such as knowledge of daily tasks that system end users will need to be able to do, should be considered in order to create a comprehensive team.

Identify funding needs

To start the project, the IDS project team should construct a preliminary budget for system creation and upkeep. As mentioned previously in this report, a survey of IDS projects found initial start-up costs to range between \$50,000 and \$800,000.

Begin researching program-specific privacy regulations

This report provides specific methods to address HIPAA and FERPA privacy regulations, however, there are many additional program-specific regulations that will need to be considered when engaging in data sharing with other agencies. A list of some of these programs is provided in Appendix B. The legal and technical personnel within the IDS team should begin researching and developing technical solutions to address these privacy regulations.

Begin modifying contracts with human services agencies to improve data quality and collection

DCDHS contracts out services to more than 300 different provider agencies. This makes standardized data collection more difficult, but also puts DCDHS in a strong negotiating position. Through the contracting process, DCDHS should work to ensure the data being collected aligns with strategic IDS goals and evaluation needs. DCDHS staff have indicated that most existing contracts adequately address data reporting requirements, but that there are still challenges with a few agencies (i.e. domestic abuse service providers and service providers who do not calculate cost per unit, etc.). DCDHS should work with these agencies, in concert with the internal IDS team, to develop data reporting requirements that satisfy all parties' needs and legal concerns.

Begin discussions with State of Wisconsin agencies

In order to ensure sustained success of an IDS program, key stakeholders must be identified. Most importantly, State of Wisconsin departments that coordinate with DCDHS and Dane County will need to be convinced of the project's value. Addressing concerns and aligning with the interests of state agencies will likely make it easier to successfully complete data sharing agreements in the long run, as the state ultimately has jurisdiction over localities. Additionally, these discussions should address the technical challenges that DCDHS and Dane County face as a result of the siloed nature of the state's data systems. This process is likely to be extremely time-consuming and should be started as soon as possible.

Mid Term (Medium Priority)

Consider hiring additional IT staff

DCDHS currently has a large backlog for IT projects. As a result, internal process flows and businesses rules rely on workarounds to achieve the intended results, and projects are continually pushed down the road. Ideally, the IT project backlog should be completed before beginning an IDS project. Existing DCDHS IT personnel have the knowledge and expertise to create an IDS system, but successful completion of the project will almost certainly require additional staff.

Funding for backlogged IT projects and additional staff could potentially be included as a part of the larger IDS project funding needs.

Establish county-wide business rules for data collection and entry

Standardized processes for data collection, cleaning, entry, and analysis should be established across all county departments. This will help to minimize errors and missing data, thereby streamlining the data merging process. Individual departments will also benefit from standardized data collection and entry processes, which are expected to decrease training requirements and reduce duplicative efforts resulting from data errors.

Develop a data sharing MOU template

Developing a data sharing MOU template that can be used with multiple organizations will dramatically reduce personnel costs downstream. The MOU should address all major privacy and security concerns, as well as major legal hurdles. DCDHS' existing contracts with human services providers can serve as a baseline for the data sharing MOU template. The template should address HIPAA and FERPA privacy regulations that are not currently covered in existing contracts. Data sharing language regarding program-specific privacy regulations (i.e. SNAP, TANF, Domestic Abuse, etc.) will likely vary depending on the agency that DCDHS/Dane County is negotiating with. Due to this variability, it will likely be more efficient to address these program-specific concerns on a case-by-case basis, rather than including them in the template.

Decide on funding strategy

Once funding needs, both long-term and short-term are identified, team members should decide on where they will seek funding. Two options presented in this document include fundraising from local organizations that support the initiative of establishing more coordinated public services, or seeking local, state, or federal funding.

Decide on system structure and design

After considering the different system structure options that are available, selecting either centrally stored data or decentralized data storage will be the first step. These decisions should be informed by conversations with current technical and budgeting staff to understand the scope of the project.

Consider a unified IT platform within Dane County and begin data sharing negotiations with other agencies

The most natural place to begin data sharing negotiations is within the Dane County government. Dane County has already awarded funding to integrate data within the criminal justice system, and an agreement with this branch of the Dane County government would provide a solid foundation for future agreements. Dane County could consider developing a single IT platform for all county services. This would increase bargaining power in negotiations with agencies outside of Dane County (i.e. more data to offer in return) and decrease the administrative burden of the negotiating process.

Long Term (Low Priority)

Engage in iterative design process

Creating a system that will meet an organization's needs will require multiple rounds of design and re-design. For this step, meet with various stakeholders for the project to establish system requirements and then design the system structure to meet those needs.

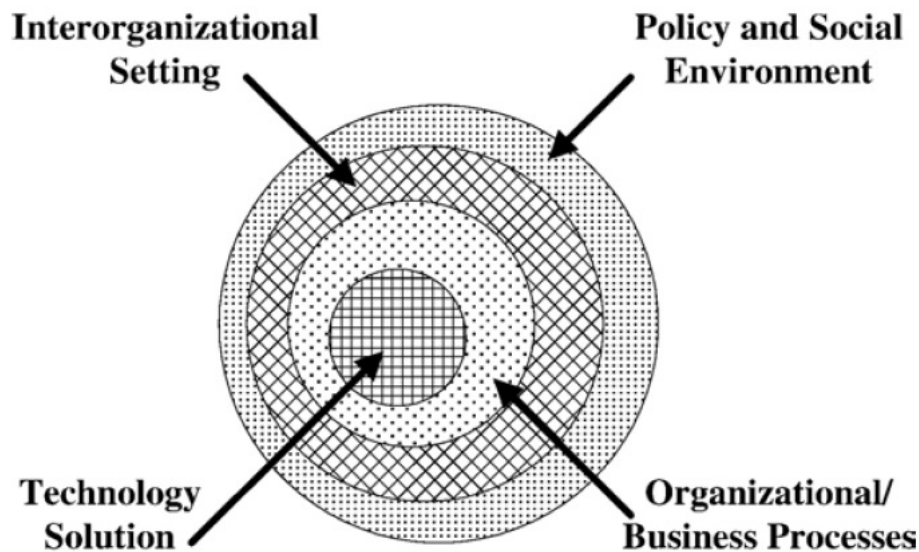
Pursue maintenance funding avenues

Regardless of what route Dane County chooses, whether funding will come from governmental organizations or local non-governmental groups, the first step will be establishing partnerships with selected groups. The organizations that provide funding should be key project stakeholders. Developing relationships and expectations early in the project will create a solid foundation for the long-term project and open up opportunities for further collaboration.

Conclusion

IDS implementation is an expensive and time-consuming endeavor, and success requires persistence, commitment, and strong leadership at multiple levels of the Dane County government. Dane County and DCDHS will need to navigate a variety of barriers in the IDS planning and implementation process, but upstream barriers are likely to be the most difficult to overcome. Data sharing agreements and will be foundational to the success of the project, and project leaders should be prepared for political, organizational, and personal resistance to IDS implementation. Managers and supervisors will need to establish strong and trusting relationships both within and outside of the organization to achieve success. The challenges of IDS implementation may seem daunting; however, integration of human services data has the potential to promote highly coordinated services, decrease costs, improve efficiency, and promote collaboration and innovation. Ultimately, successful IDS projects can improve the lives and health outcomes of both the super-utilizer population and the community as a whole. If the challenges to IDS implementation can be successfully navigated, Dane County and DCDHS could serve as a pilot for future IDS projects, laying the groundwork and providing a roadmap that can be applied throughout the state.

Appendix A: Information Integration Framework



Source: Pardo and Tayi (2007)

Technical Context

The technical context refers to the technological improvements organizations make to increase productivity and provide better services. This could be new intra-office messaging software, updating or upgrading email services, a redesign of cost accounting practices, or a full database overhaul. In the specific case of DCDHS, this context encompasses the software and hardware of IDS, as well as the coding solutions and data requirements needed for the platform to work. This context draws on the expertise of information technology (IT) personnel and experts in computer science and related fields.

Organizational Context

The organizational context refers to anything that falls within the environment of an organization. This includes standard operating procedures, common practices, organizational hierarchy and structure, and organizational culture. This context draws on the fields of management and public administration for theory and perspective.

Interorganizational Context

The interorganizational context refers to the interactions between organizations. Again, this context draws heavily from the fields of management and public administration, but also incorporates some of the perspectives of political science and public policy. It is expected that the challenges associated with this context will be crucial in the early stages of IDS implementation, when DCDHS will need to begin coordinating with other Dane County agencies.

Political/Social Context

The political and social context refers to the legal, social, and policy environments that organizations must operate within. This context is very difficult for a single organization to change and draws on a wide variety of fields, including political science, psychology, and behavioral economics. It is important that administrators understand how their organizations and proposed projects are positioned within this broader context.

Appendix B: Legal Resources

HIPAA Resources

- HIPAA (Protected Health Information) HHS guidance to covered entities: <https://www.resdac.org/cms-data/request/cms-virtual-research-data-center>
- HHS/Department of Education guidance to relationship between FERPA and HIPAA: <http://www.cumc.columbia.edu/hipaa/docs/ferpa-hippa-guidance.pdf>
- National Institutes of Health discussion of clinical research and Privacy Rule: http://privacyruleandresearch.nih.gov/pr_02.asp
- Office for Civil Rights discussion of HIPAA and research: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/research.html>
- HHS discussion of de-identification of health information: <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/>
- Centers for Medicare and Medicaid Services data use agreement: <https://www.cms.gov/cmsforms/downloads/cms-r-0235.pdf>
- North Carolina Department of Health and Human Services data use agreement for a limited data set: https://www2.ncdhhs.gov/info/olm/manuals/dhs/pol-80/man/DHHS_Data_Use_Agreement_Template.pdf
- University of Buffalo’s explanation for why business associate agreements are not required for researchers: <http://www.hpitp.buffalo.edu/hipaa/Research/DataExtraction.htm>

HHS discussion of business associates, noting that researchers are not required to enter business associate agreements for the purpose of accessing protected health information for research: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es>

FERPA Resources

- U.S. Department of Education guidance on FERPA and resources: <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- HHS/Department of Education guidance to relationship between FERPA and HIPAA: <http://www.cumc.columbia.edu/hipaa/docs/ferpa-hippa-guidance.pdf>
- U.S. Department of Education guidance on protection of human subjects: <http://www2.ed.gov/about/offices/list/ocfo/humansub.html>
- U.S. Department of Education sample agreement between educational institution and authorized representative: <http://www2.ed.gov/about/offices/list/ovae/pi/cte/uiferpa.html>
- Amended FERPA regulation permitting data sharing agreements with entities not under “direct control” of the educational institution: <http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf>
- National Center for Educational Statistics guide to privacy and confidentiality of educational records: <http://nces.ed.gov/pubs2011/2011601.pdf>
- Privacy Technical Assistance Center guidance on IDS and student privacy: <http://ptac.ed.gov/sites/default/files/IDS-Final.pdf>

42 CFR Part 2 (based on version prior to January 13, 2017)

- Discussion of the relationship between the HIPAA Privacy Rule and 42 CFR: http://publichealth.gwu.edu/departments/healthpolicy/CHPR/downloads/behavioral_health/bhib-18-19.pdf
- FAQs on the regulation maintained by the U.S. Substance Abuse and Mental Health Services Administration: <http://www.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs>
- National Center for State Courts: Future Trends in State Courts: 42 CFR Part 2: http://www.ncsc.org/sitecore/content/microsites/futuretrends2012/home/PrivacyandTechnology/-/media/Microsites/Files/Future%20Trends%202012/PDFs/SubstanceAbuse_Kunkel.ashx

HMIS (Homeless Management Information System)

- Overview of the HMIS prepared by the U.S. Department of Housing and Urban Development: <https://www.hudexchange.info/programs/hmis/>
- Overview of data elements that must be collected by HMIS programs: <https://www.hudexchange.info/resource/3826/hmis-data-standards-manual/>
- Discussion with example of HMIS research agreements: <https://www.hudexchange.info/resources/documents/ModelHMISResearchAgreement.pdf>
- Discussion of de-identified protected personal information (PPI) in the HMIS system: <https://www.hudexchange.info/resource/1314/guidelines-unduplicating-and-deidentifying-hmis-client-records/>

Privacy Act of 1974

- U.S. Department of Education requirements for Privacy Act matching agreements: <http://www2.ed.gov/policy/gen/leg/foia/acsom6105.pdf>

Law enforcement data and criminal justice settings

- Analysis of use of arrest and related records prepared by the U.S. Department of Justice Bureau of Justice Statistics: <https://www.bjs.gov/content/pub/pdf/umchri01.pdf>
- State laws on juvenile interagency information sharing: <https://www.ncjrs.gov/pdffiles1/ojjdp/215786.pdf>
- Guide to Michigan law and court rules on accessing court records and filings: <http://courts.mi.gov/administration/admin/op/pages/records-management.aspx>
- An overview of information sharing in court-related projects: https://www.bja.gov/publications/csg_cjmh_info_sharing.pdf

Enforcement of Privacy and Confidentiality Laws

- The HHS Office of Civil Rights is primarily responsible for enforcing HIPAA. It maintains a website on its enforcement activities here: <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html>
- The U.S. Department of Education’s Family Compliance Office has primary responsibility for enforcing FERPA violations. Its website is here: <https://www2.ed.gov/policy/gen/guid/fpco/index.html?exp=0>

Appendix C: Sample Data Sharing Agreements

The following pages include complete samples of data sharing memoranda of understanding (MOUs) from a variety of sources. The samples include an agreement between Allegheny County and multiple school districts, key confidentiality provisions outlined by District of Columbia Public Schools (DCPS), a global MOU regarding child welfare services in California, an inter-agency data exchange agreement in New York City, and an MOU regarding services for children in Jefferson County, Colorado.

Sample MOU with annotation

	Question	Additional Information
20	If consent is specifically addressed in statute, regulation, administrative policy, or other, describe how it applies to the specific data (e.g., categories or type of data to which consent applies, time periods, expiration data, how data collected prior to consent authorization are addressed.)	
21	Does the scope of the legal, regulatory, administrative policy or other specifically address minors?	Yes, No. If yes, provide cite and requirements.
22	Does the scope of the legal, regulatory, administrative policy or other address individuals who are not competent to consent?	Yes, No. If yes, provide cite and requirements.
23	Does the agency have any existing memoranda of understanding (MOUs) with other agencies, contractors, or third parties related to data sharing?	Yes, No. If yes, provide list and attach copies.
24	Does the scope of the legal, regulatory, administrative policy, or other specifically address utilization of data for research and requisite protocols?	Yes, No. If yes, provide citations and specify requirements.

The following template can be used for drafting an MOU between the Lead IDS Agency and the Data Contributor(s). No single paragraph is required in all MOUs. The length, formality, and comprehensiveness of the document and language may vary depending on organizational legal culture. Even the name given to the agreement may vary depending on jurisdiction.

*Note that format/structure and some content are from Cornman (2009).

Example Text/Content of MOU Document	Comments*												
<p>1. Title</p> <p>Data Sharing MOU establishing the Tri-state Partnership Group</p>	<p>Principles: Provide a descriptive title that clarifies purpose of MOU and makes it easily distinguishable from other agreements between the parties.</p>												
<p>2. Parties to the MOU</p> <table><tr><td>Date Source Name:</td><td>Lead IDS Agency Name:</td></tr><tr><td>Primary Contact Person:</td><td>Primary Contact Person:</td></tr><tr><td>Title:</td><td>Title:</td></tr><tr><td>Address:</td><td>Address:</td></tr><tr><td>Telephone:</td><td>Telephone:</td></tr><tr><td>E-mail Address:</td><td>E-Mail Address:</td></tr></table>	Date Source Name:	Lead IDS Agency Name:	Primary Contact Person:	Primary Contact Person:	Title:	Title:	Address:	Address:	Telephone:	Telephone:	E-mail Address:	E-Mail Address:	<p>Principles: This section documents the legal names and contact information of the parties.</p> <p>Practice Recommendations: Changes to this information must be made via written notification and amendment. Since there may be multiple agreements between parties, contact information should be as specific as possible and identify principal contact persons at each entity.</p>
Date Source Name:	Lead IDS Agency Name:												
Primary Contact Person:	Primary Contact Person:												
Title:	Title:												
Address:	Address:												
Telephone:	Telephone:												
E-mail Address:	E-Mail Address:												

(Continued on following 11 pages)

Example Text/Content of MOU Document	Comments*
<p>3. Principles for MOU</p> <p>Basic Principles for this MOU:</p> <ul style="list-style-type: none">Electronic storage of data and information is ubiquitous in today’s society and continues to be created, stored, and shared at an expansive pace;There is a presumption that as long as certain protective structures are in place, restrictions on sharing such data should only be observed when there is a clear legal bar to such sharing;There is a strong consensus in favor of systematically integrating data and information systems in order to improve the process of policy making and implementation of programs for governmental/public purposes;Such integrated data systems (IDS) are not only appropriate and legal, but can provide essential capabilities in furthering the core governmental functions of audit, evaluation, and research in public programs and policy;The IDS supported by this MOU creates clear rules and processes that govern who, when, how and why individuals and entities can access data for public use, as well as ensure compliance with regulatory and oversight structures, and to address any confidentiality and privacy concerns; <p><Additional principles as desired for specific MOU relationship></p> <p>With the intent to be legally bound hereby, the parties to this MOU set forth the following as terms and conditions of their understanding.</p>	<p>Principles: Should identify specific guiding principles of the interagency data agreement.</p> <p>Practice Recommendations: May wish to be more formal using “whereas” statements. May want to also note more generally that an MOU describes the relationships between, and responsibilities of, the parties who have agreed to share data.</p>
<p>4. Background, Purpose, and Scope</p> <p><Name of Data Contributor> is responsible for providing and administering services for residents of _____. It is dedicated to meeting those needs and most particularly to the state’s most vulnerable populations, through an extensive range of prevention, intervention, crisis management, and after care services provided through its program offices. Services include: _____.</p> <p><Name of Data Contributor> believes that sharing certain data can be beneficial for served populations and improve state programs and services. The goal is to increase data use for policy, evaluation, and research to better serve the vulnerable populations of our state.</p> <p><Additional Background and definition for scope of agreement as desired></p>	<p>Principles: Provide context for the agreement. Identify specific purpose of the agreement, and define and limit the scope of specific data sharing relationship.</p> <p>Practice Recommendations:</p> <ol style="list-style-type: none">Briefly describe relationship between the agencies and explain how work described in this agreement will benefit the relationship. Also include short history of the relationship.May include information about the functions of the different parties involved.May include whereas clause information/principles.May want to include structure of IDS here (if not below).May want the purpose and scope in separate section if desired.

Example Text/Content of MOU Document	Comments*
<p>5. Glossary/Definitions of Terms</p>	<p>Principles: Define key terms in this agreement.</p> <p>Practice Recommendations: Include even standard terms if there is potential for misinterpretation.</p>
<p>6. Legal Authority</p> <p><Name of Data Contributor> has legal authority to enter into this agreement and share data covered by this MOU with the <Lead IDS Agency>, including disclosure and re-disclosure, under sections _____ of the state of _____ statutes. . . . It is understood that shared data may be re-disclosed with other end users under the terms defined below.</p>	<p>Principles: Establish that parties have the legal authority to act, make decisions, enforce decisions, and/ or enter into an agreement. Establish that under the terms of this MOU, administrative data will be shared by the parties pursuant to (insert statute). This MOU is intended to facilitate information sharing between the parties</p> <p>Practice Recommendations: Should speak to the specific authority that allows for the establishment of the IDS that includes language around discretion to disclose/re-disclose/mandate and discretion to evaluate/mandate to evaluate. Should cite specific statutes, executive orders, disclosure laws, paperwork reduction acts, etc. May also want to discuss Ownership issues here (if not below).</p>
<p>7. Data to Be Shared</p> <p><Name of Data Contributor> will provide the following data to the <Lead IDS Agency>:</p> <ul style="list-style-type: none">a. Statewide Medicaid enrollment records for 2010-2016;b. Statewide Medicaid Service Claims records for 2010-2016;c. Statewide Medicaid MCO shadow claims 2010-2016;d. Statewide Medicaid Pharmacy claims for 2010-2016;e. Etc.	<p>Principles: Describe in detail the data that will be shared by the Data Contributor.</p> <p>Practice Recommendations: May wish to just broadly describe the data to be shared and then refer to a separate document or appendix that specifies the databases, elements/items, and formats, as well as other parameters such as geographic boundaries and dates ranges.</p>

Example Text/Content of MOU Document	Comments*
<p>8. Ownership</p> <p>This MOU does not constitute a transfer of any title or interest in the Data, and <Name of Data Contributor> reserves all rights in the Data not expressly granted to <Lead IDS Agency> by this agreement. Any portion of the Data that is modified or merged into another form or merged with other Data shall continue to be subject to the provisions of this agreement.</p> <p><Name of Data Contributor> makes no guarantee as to the accuracy or currency of the Confidential Information that will be provided as a result of this MOU.</p> <p>The person who will be the data custodian at <Lead IDS Agency>, and will be responsible for ensuring that the provisions of this agreement are carried out, is:</p> <p>Name Title Address Phone E-mail Address</p> <p>Alternate Contact:</p> <p>Name Title Address Phone E-mail Address</p>	<p>Principles: Should set forth the ownership rights and responsibilities for the data that are subject to the MOU. Should also specify the custodian of the shared data (including contact information).</p> <p>Practice Recommendations: Address:</p> <ol style="list-style-type: none">Operational impact questions:<ol style="list-style-type: none">Who is responsible for veracity?Who is responsible for security?Who is responsible for updates?If there is a HIPAA violation, who is responsible?Structure of IDS may be important here.May want to consider copyright laws, intellectual freedom, and recent SCOTUS rulings around this. <p>Some MOUs contain disclaimer language such as: “Parties to this MOU do not make any representation or warranty, express or implied, as to the accuracy or completeness of any furnished information or other due diligence materials, and no Party, or any of its directors, trustees, officers, employees, shareholders, owners, affiliates, representatives, or agents, has or will have any liability to any other Party or person resulting from any reliance upon or use of, or otherwise with respect to, any furnished information or other due diligence materials.”</p> <p>Or: “Only those representations or warranties made expressly in a data use agreement or in any binding agreements pertaining to the IDS, when, as, and if it is executed, and subject to such limitations and restrictions as may be specified in such agreement, will have any legal effect.”</p>

Example Text/Content of MOU Document	Comments*
<p>9. IDS Structure</p> <p>The IDS structure maintained at the <Lead IDS Agency> follows a federated/ non-federated model where data are . . .</p>	<p>Principles: Describe structure of IDS (if not laid out above).</p> <p>Practice Recommendations: Describes federated vs. non-federated models, as well as the governance structure. Use of graphics and schematics can help in the understanding of the structure.</p> <p>This section may also address data security and confidentiality/privacy—if not covered separately below.</p>
<p>10. Roles and Responsibilities</p> <p>In accordance with the provisions of this agreement:</p> <p>A. The <Name of Data Contributor> will be responsible for:</p> <ol style="list-style-type: none">Compiling the shared data and facilitating its transfer to <Lead IDS Agency>Providing ongoing assistance in the integration and analysis of data, as well as interpretation of findings/resultsEtc. <p>B. The <Lead IDS Agency> will be responsible for:</p> <ol style="list-style-type: none">Securing and using the shared data;Informing <Name of Data Contributor> of disclosures, findings, and disposition of the Data;Etc.	<p>Principles: Clearly describe and delineate the agreed upon roles and responsibilities each organization or agency will be providing to ensure project success.</p> <p>Practice Recommendations: The roles and responsibilities should align with project goals, objectives, and target outputs.</p> <p>May want to include specific reference to the databases that will be used and the authorized studies that will be undertaken e.g., refer to the record layout. Some agreements have the record layouts in the appendix. Reference to specific studies may be better included in the Data Use and Permissions section below.</p>
<p>11. Funding Information and Costs of Reimbursement</p> <p>This is a reciprocal data sharing agreement between <Name of Data Contributor> and <Name of Lead IDS Agency>, and both parties acknowledge the benefit of the availability of integrated data via the <Name of Lead IDS Agency> resource. As a result, neither party will charge the other party for the use of and access to data to be exchanged pursuant to this MOU, except as otherwise provided herein.</p>	<p>Principles:</p> <p><i>Funding:</i> If funds are to be obligated under the agreement, the financial arrangements to all parties must be clearly stipulated. If no funds are obligated under the agreement, a statement should be included that makes it clear that the agreement is not an instrument that obligates funds of any party to the agreement.</p> <p><i>Costs and reimbursement:</i> If the agreement results in the exchange of money between agencies, state the estimated cost or costs not to exceed, terms of payments, and dispute resolution conditions.</p> <p>Practice Recommendations: May include how downstream revenue is to be handled if there is re-use of data. May also include discussion of how IDS structure impacts funding and reimbursement. May also include differential pricing.</p>

Example Text/Content of MOU Document	Comments*
<p>12. Confidentiality and Privacy</p> <p>Parties understand that disclosure and re-disclosure of the Confidential Information is governed by both federal and state law. For example (and not by way of limitation), federal restrictions on this information are contained in 42 U.S.C. § 503, 26 U.S.C. § 3304, and subpart B of 20 C.F.R. Part 603, and the Family Educational Rights and Privacy Acts Statute (“FERPA”) against unauthorized access or re-disclosure. State law restrictions are contained in _____. Pursuant to these requirements, the parties (and each person having access to the data), covenant as follows, and agree that upon their receipt of any Confidential Information, they are representing that they have complied with and/or have accomplished, and will continue to comply with and accomplish each of the following:</p> <p>1. Confidential Information will be used only for the purposes authorized by law and only for the purposes specified in this MOU;</p> <p>2. Access to Confidential Information will be provided only to authorized personnel who are required to perform activity required by this MOU and who need to access it for purposes listed in this MOU, who have executed a confidentiality certification. A signed copy of the Certification shall be provided by the individual who signs this MOU;</p> <p>3. Parties will instruct all Authorized Personnel as to the confidential nature of all Confidential Information, the safeguards required to protect the information, the civil and any criminal sanctions for non-compliance pursuant to state laws.</p> <p>4. Parties and Authorized Personnel will strictly adhere to the requirements of this MOU and its required procedures, and will report any breaches fully and promptly;</p> <p>5. Parties will take precautions to ensure that only authorized personnel have access to the computer systems in which the Confidential Information is stored;</p> <p>6. Parties will implement safeguards and precautions to ensure that only Authorized Personnel have access to the Confidential Information;</p> <p>7. Parties will ensure that Confidential Information will be stored in a place physically secure from access by unauthorized persons;</p> <p>8. Parties will ensure that Confidential Information in electronic format is stored and processed in such a way that unauthorized persons cannot retrieve the information by means of computer or otherwise gain access to it;</p> <p>9. Parties shall immediately terminate an individual's authorized access upon changes in the individual's job duties that no longer require access, unauthorized access to, or use of Confidential Information by the individual, or termination of employment; and</p> <p>10. Parties shall transmit the Confidential Information by a secure method and encrypt all personally identifiable information (PII) during receipt, transmission, storage, maintenance, and use.</p>	<p>Principles: Address how privacy will be ensured and how confidential information will be protected (if not addressed above in IDS description).</p> <p>Practice Recommendations:</p> <p>Confidentiality, privacy, and data security are all separate issues.</p> <p>1. <i>Confidentiality</i> refers to that which is done in confidence with the expectation of privacy</p> <p>2. <i>Privacy</i> means the right to restrict access to private information</p> <p>3. <i>Data security</i> is separate section</p> <p>Should identify the relevant statutes on confidentiality. Discuss issues of training, access, and storage and who is responsible for training, access, and storage. Discuss how to address state law and how to deal with pre-emption. May want to require compliance with any oversight boards (e.g., IRB) and stipulate that individuals who are approved to work on joint projects to be trained on safeguard to protect confidential information.</p> <p>Reference relevant statutes: e.g., HIPAA; FERPA; The Common Rule; Privacy Act of 1974; 42 CFR; HMIS; Children’s Online Privacy Act; Child Abuse Prevention and Treatment Act.</p>

Example Text/Content of MOU Document	Comments*
<p>13. Data Security</p> <p><Name of Lead IDS Agency> will use appropriate safeguards to prevent use or disclosure of the individually identifiable information other than as provided for by this Agreement.</p> <p><Name of Lead IDS Agency> maintains and uses appropriate administrative, technical, and physical safeguards to preserve the integrity and confidentiality of the IDS and to prevent non-permitted use or disclosure of individually identifiable information.</p> <p><Name of Lead IDS Agency> will ensure that any agent, including a subcontractor, to whom it provides individually identifiable information, received from, or created or received by <Name of Lead IDS Agency>, executes a written agreement obligating the agent or subcontractor to comply with all the terms of the Agreement.</p>	<p>Principles: Includes policies and procedures to protect the confidentiality and safety of data.</p> <p>Practice Recommendations:</p> <p>Discuss:</p> <p>1. who is responsible for data security;</p> <p>2. who is responsible for keeping data-use agreements; what records should be retained; back-up systems; the duration of time that records should be retained</p> <p>3. specific protocols for physical and virtual/electronic security—be specific about proposed security arrangements and demonstrate full understanding of applicable statutes, regulations, and traditional practices;</p> <p>4. how data security changes with industry standards (consider resources such as the SANS Institute [sans.org] and CERT at Carnegie Mellon University [cert.org])</p> <p>5. how parties can inspect security arrangements for the purpose of confirming the user is in compliance with data security procedures and requirements specified by the agreement.</p>

Example Text/Content of MOU Document	Comments*
<p>14. Data Use, Permissions, and Retention</p> <p>A. Data will be transferred to/accessed by <Name of Lead IDS Agency> using the following secure procedures: . . .</p> <p>B. Permissions and consents to use the data will be provided by the <Name of Data Contributor> or obtained by <Name of Lead IDS Agency> to comply with any applicable state or federal laws and/or regulations prior to <Name of Data Contributor> furnishing individually identifiable information pertaining to an individual.</p> <p>C. <Name of Lead IDS Agency> shall use or disclose the shared data only for the purposes of:</p> <p>D. <Name of Lead IDS Agency> will not use or disclose individually identifiable information other than as permitted or required by this Agreement, or as required by state and federal law, or as otherwise authorized by data owners.</p> <p>E. <Name of Lead IDS Agency> agrees <u>not</u> to perform any of the following actions:</p> <p> a. Attempting to identify any individual whose health information is included in a de-identified Limited Data Set.</p> <p> b. Using or further disclosing any data for any purpose other than the purpose specified above or as otherwise permitted by law.</p> <p> c. Publishing or otherwise disclosing information that identifies the individuals whose health information is included in shared data.</p> <p>F. <Name of Lead IDS Agency> agrees not to use or permit others to use shared data that identify an entity or individual health care provider for any of the following purposes:</p> <p> a. To compete commercially against an entity.</p> <p> b. To determine the rights, benefits, or privileges of an entity or individual health care provider.</p> <p> c. To report, through any medium, information that identifies an entity or individual health care provider.</p> <p>G. <Name of Lead IDS Agency> will use appropriate safeguards to prevent use or disclosure of the individually identifiable information other than as provided for by this Agreement. <Name of Lead IDS Agency> will develop, implement, maintain, and/or use appropriate administrative, technical, and physical safeguards to preserve the integrity and confidentiality of and to prevent non-permitted use or disclosure of individually identifiable information. These safeguards are required regardless of the mechanism used to transmit the information. <Name of Lead IDS Agency> will document and keep these safeguards current.</p> <p>H. Shared data will be retained by <Name of Lead IDS Agency> for the duration of this agreement and any renewals of this agreement. Back-up systems will be implemented according to industry standards to appropriately secure the back-up media/files. Upon termination of this agreement, shared data and back-up files will be permanently deleted (e.g., using overwrite protocols) within 90 days of the termination date. This requirement applies to all end users with whom data was shared by <Name of Lead IDS Agency>. <Name of Lead IDS Agency> is responsible for providing confirmation of such data destruction.</p>	<p>Principles: Define the scope and process of using data, as well as data transfer protocols.</p> <p>Practice Recommendations:</p> <p>Describe issues such as:</p> <p> 1. How the data will be securely transferred (or accessed if a federated structure).</p> <p> 2. Record usage, duplication, and re-disclosure restrictions: limitations on the access to, disclosure, and use of information. Who can access the data? Limitations on identifiable data? Where can research/analysis be done?</p> <p> 3. Use of administrative data for other projects: specify the project and/or uses which the other agency can use administrative records.</p> <p> 4. Data available for researchers: Consider whether the data subject to these administrative records will be made available to researchers or to the public. Are restricted data use licenses implicated? What kind of public disclosures need to be made?</p> <p> 5. Describe any required statutory firewalls.</p> <p> 6. Data retention—including what records shall be retained for the project contemplated by the agreement and for a back-up system. Specify the duration of time that records should be retained.</p>

Example Text/Content of MOU Document	Comments*
<p>15. Notification of results, dissemination of results, and dissemination of end products.</p> <p><Lead IDS Agency> will notify and provide draft copies of results and findings derived from analyses of contributed data produced by <Name of Lead IDS Agency>, its employees, subcontractors, agents, or end Data Licensees. Such results and end product must be provided to the <Name of Data Contributor> no less than 30 days prior to the dissemination of such results or products. Such notice should be provided to the following individuals at <Name of Data Contributor>:</p> <p> Name Title Address Phone E-mail Address</p> <p> Alternate Contact:</p> <p> Name Title Address Phone E-mail Address</p> <p><Name of Data Contributor> will then have 30 days to offer relevant review for accuracy, appropriate citations, etc., and acknowledgment of the results or products. <Name of Lead IDS Agency> may presume acknowledgment if none is forthcoming within the 30-day review period.</p>	<p>Principles: Describe protocols for providing notice of dissemination of findings from data analyses.</p> <p>Practice Recommendations: If the parties are releasing any documents or research related to the exchange of administrative data, specify the subject matter, rights, and responsibilities pertaining to the public use of data. Data citations should also be discussed here as well as definitions for documenting data linking and cleaning process.</p> <p>May also wish to include provisions for an evaluation of the Lead IDS Agency process and use of the shared data, if desired.</p>
<p>16. Notification if signatories are deleted from or added to the agreement</p> <p><Name of Lead IDS Agency> is responsible for notifying <Name of Data Contributor> and all signatories to this agreement of any additional signatories, deleted signatories, or other data contributors no more than 30 days after the final execution of relevant documents.</p>	<p>Principles: Define who is responsible for notifying the original signatories about additional/deleted signatories or data contributors.</p>
<p>17. Term of Agreement</p> <p>This MOU will be effective on the date that the last Party has executed it (the “Effective Date”), and shall terminate on the date that is five (5) years from the Effective Date, unless such term is extended by mutual agreement.</p>	<p>Principles: State specific start and end dates of MOU.</p> <p>Practice Recommendations: If the completion date is not known and the period of the agreement is expected to stretch over a number of years, the completion date may be listed as indefinite.</p>

Example Text/Content of MOU Document	Comments*
<p>18. Performance Standards and Review Procedures</p> <p><Name of Lead IDS Agency> understands that <Name of Data Contributor> and other statutory authorities have the right to audit <Name of Lead IDS Agency>'s policies, procedures, and implementation of those policies and procedures for safeguarding the shared data and preserving the confidentiality of information. In addition, <Name of Data Contributor> shall be permitted to audit and monitor <Name of Lead IDS Agency>'s and its employees' access to and use of the Confidential Information on a periodic and "as needed" basis, including on-site inspections, to determine compliance with this MOU. <Name of Lead IDS Agency> agrees to cooperate fully with any auditing or on-site inspections. All reasonable costs of the auditing authority for such auditing and inspection shall be the sole expense of <Name of Data Contributor>. <Name of Lead IDS Agency> shall create and maintain a system sufficient to allow an audit of compliance with the requirements of this MOU.</p>	<p>Principles: If the agreement is extended for an indefinite period of time, it should contain a provision for review, at least every three years, to determine the continuing need and whether the agreement should be revised, renewed, or cancelled.</p> <p>Practice Recommendations: Should include provisions for audits:</p> <ol style="list-style-type: none">1. Should specify who is responsible for audit2. Should specify the components of the audit report (citing strengths, deficiencies, and any corrective actions that need to be taken)
<p>19. Resolution of Conflicts</p> <p>In the event a party to the MOU believes that a provision of the MOU has been breached, or if there is a disagreement regarding implementation of the MOU or any of its provisions, the parties agree to attempt to resolve the conflict in the following manner:</p>	<p>Principles: Set forth the method for settling disputes.</p> <p>Practice Recommendations:</p> <ol style="list-style-type: none">1. Describe process that will occur if a party to the agreement breaches the agreement2. Issues/events that give rise to a breach of the agreement, at least in general detail.

Example Text/Content of MOU Document	Comments*
<p>20. Unauthorized disclosure of information or other breach</p> <p><Name of Lead IDS Agency> will report to <Name of Data Contributor>, in writing, any use and/or disclosure of individually identifiable information that is not permitted or required by this Agreement of which <Name of Lead IDS Agency> becomes aware. Such report shall be made as soon as reasonably possible but in no event more than ten (10) business days after discovery by <Name of Lead IDS Agency> of such unauthorized use or disclosure. This reporting obligation shall include breaches by <Name of Lead IDS Agency>, its employees, subcontractors, agents, or end Data Licensees. Each such report of a breach will:</p> <ol style="list-style-type: none">a. identify the nature of the non-permitted use or disclosure;b. identify the individually identifiable information used or disclosed;c. identify who made the non-permitted use or disclosure;d. identify who received the non-permitted use or disclosure;e. identify what corrective action <Name of Lead IDS Agency> took or will take to prevent further non-permitted uses or disclosures;f. identify what <Name of Lead IDS Agency> did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; andg. provide such other information as <Name of Data Contributor>, or the data owners, may reasonably request. <p><Add indemnification and/or liquidated damages language></p>	<p>Principles: Specify the remedies and damages in the event of a breach of contract by any party to the agreement or unauthorized disclosure of data.</p> <p>Practice Recommendations: Describe:</p> <ol style="list-style-type: none">1. the responsibilities for notification by points of contact of each party the MOUs.2. any criminal/civil penalties that may apply for unauthorized disclosure of information.3. indemnification language and limitations of liability.4. any liquidated damages for breach of agreement if applicable. <p>May want to specify Parties negotiating an agreement often make an explicit agreement as to what each party's remedy for breach of contract shall be.</p>
<p>21. Supersedes</p> <p>This MOU <u>supersedes</u> any previous understandings, representations, or agreements, whether written or oral, that may have been made or entered into by the parties relating to the subject matter hereof.</p> <p>OR</p> <p>This MOU does <u>not supersede</u>, replace, or render invalid any other agreement. The Participants mutually agree to promote and advance the purpose of this MOU to enhance information sharing, when necessary, beyond any existing understandings or agreements, including this one.</p>	<p>Principles: Establish relationship of this agreement with other understandings or agreements between the parties.</p>
<p>22. Severability</p> <p>Nothing in this MOU is intended to conflict with the current laws, regulations, or policies applicable to each Party. If a term of this MOU is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOU shall remain in full force and effect.</p>	<p>Principles: Establish severability of terms of the MOU.</p>

Example Text/Content of MOU Document	Comments*
23. No Private Right of Action This agreement does not create any private cause of action for enforcement or damages.	Principles: Clarify that the MOU does not create a private right of action.
24. Modification/Amendment of the MOU Modifications or Amendments to this MOU must be in writing and formally agreed to/executed by all Parties. Concurrence provisions below apply. OR There shall be no modifications or amendments of this MOU, except in writing, executed with the same formalities as this instrument.	Principles: Set forth the process for amending the MOU. Practice Recommendations: Amendments should be with consent of all parties to the MOU and in writing.
25. Termination of the MOU. Either party may, with or without cause, terminate this MOU by giving a ninety (90) day written notice of its intent to do so. In the event changes in either state or federal law or regulations occur which render performance hereunder illegal, void, impracticable, or impossible, this MOU shall terminate immediately; however, obligations with respect to the treatment and security of Confidential Information and shall survive any termination of this MOU.	Principles: Set forth process for termination of the MOU. Practice Recommendations: Should contain a provision whereby each party may terminate the agreement within a specified time frame
26. Concurrence	Principles: In order to be a valid agreement, there must be concurrence by all parties to the agreement. Practice Recommendations: Identify the agency signatories. Agency signatories agree that they have the authority to sign for the agency or participating entity and denote their acceptance of the agreement terms by affixing their signature and the date.

* Note that format/structure and some content of comments is taken from “The Unique Method for Obtaining Data: Model Agreement to Share Administrative Records,” published by the *Federal Committee on Statistical Methodology*, July 2009.

Example Text/Content of DUL Document	Comments*
1. Title Data Use License for the Smith Research Group	Principles: Provide a descriptive title that clarifies purpose of DUL and makes it easily distinguishable from other agreements between the parties.
2. Parties to the DUL Lead IDS Agency Name: Data Licensee Name: Primary Contact Person: Primary Contact Person: Title: Title: Address: Address: Telephone: Telephone: E-mail Address: E-Mail Address:	Principles: This section documents the legal names and contact information of the parties. Practice Recommendations: Changes to this information must be made via written notification and amendment. Note as there may be multiple agreements between parties, contact information should be as specific as possible and identify principle contact persons at each entity.

(Continued on following 11 pages)

Sample DUL with annotation

Example Text/Content of DUL Document	Comments*
<p>3. Principles for Data Use License (DUL)</p> <p>Basic Principles for this DUL:</p> <ul style="list-style-type: none">• Electronic storage of data and information is ubiquitous in today’s society and continues to be created, stored, and shared at an expansive pace;• There is presumption that as long as certain protective structures are in place, restrictions on sharing such data should only be observed when there is a clear legal bar to such sharing;• There is a strong consensus in favor of systematically integrating data and information systems in order to improve the process of policy making and implementation of programs for governmental/public purposes;• Such integrated data systems (IDS) are not only appropriate and legal, but can provide essential capabilities in furthering the core governmental functions of audit, evaluation, and research in public programs and policy;• This Data Use License Agreement (DUL) is intended to allow limited use of specific IDS data and creates clear rules and processes that govern who, when, how, and why individuals and entities can access data for specified uses, as well as ensure compliance with regulatory and oversight structures, and to address any confidentiality and privacy concerns; <p><Additional principles as desired for specific DUL Relationship></p> <p>With the intent to be legally bound hereby, the parties to this DUL set forth the following as terms and conditions of their understanding.</p>	<p>Principles: Should identify specific guiding principles of the interagency data use license.</p> <p>Practice Recommendations: May wish to be more formal using “WHEREAS” statements. May want to also note more generally that an DUL describes the relationships between, and responsibilities of, the parties who have agreed to share data.</p>
<p>4. Background, Purpose, and Scope</p> <p><Name of Lead IDS Agency> has entered into MOUs with data owners, and compiled and linked several data systems into an organized IDS. It is dedicated to encouraging access and use of the IDS for policy, evaluation, research, and audit purposes while protecting the rights of individuals whose data is contained in the IDS under all applicable state and federal laws. <Name of Lead IDS Agency> accomplishes this by providing access to limited data sets and/or de-identified data to responsible and credible entities through execution of legally binding data use license agreements.</p> <p><Data Licensee> conducts evaluations and research in the areas of _____ and desires to continue such work through accessing data contained in the <Name of Lead IDS Agency> IDS. The specific objectives and purpose of the proposed access and analyses are: _____. Anticipated analyses of the data and products will include _____. No additional analyses or products (other than those explicitly outlined above) will be pursued without explicit written permission of <Name of Lead IDS Agency>.</p> <p><Additional Background and definition for scope of agreement as desired></p>	<p>Principles: Provide context for the agreement. Identify specific purpose of the agreement, and define and limit the scope of specific data sharing relationship.</p> <p>Practice Recommendations:</p> <ol style="list-style-type: none">1. Briefly describe relationship between the agencies and explains how work described in this agreement will benefit the relationship. Also include short history of the relationship.2. May include information about the functions of the different parties involved.3. May include whereas clause information/principles4. May want to include structure of IDS and data to be accessed here (if not below) <p>May want the Purpose and scope in separate section if desired.</p>

Example Text/Content of DUL Document	Comments*
<p>5. Glossary/Definitions of Terms</p> <p>Lead IDS Agency –</p> <p>Data License –</p> <p>Custodian –</p> <p>Etc.</p>	<p>Principles: Define key terms in this agreement.</p> <p>Practice Recommendations: Include even standard terms if there is potential for misinterpretation.</p>
<p>6. Legal Authority</p> <p><Name of Lead IDS Agency> has legal authority to enter into this agreement and share data covered by this DUL with the <Data Licensee>, including disclosure and re-disclosure, under legally binding Memoranda of Understanding with Data Owners and under applicable sections of state and federal laws. . . . It is understood that shared or accessed data may <u>not</u> be re-disclosed by <Data Licensee> with other end users without explicit written permission of <Name of Lead IDS Agency>.</p>	<p>Principles: Establish that parties have the legal authority to act, make decisions, to enforce decisions, and/ or enter into an agreement. Establish that under the terms of this DUL, administrative data will be shared by the parties pursuant to (insert statute) This DUL is intended to facilitate information sharing between the parties for the specific purposes outlined in the agreement only.</p> <p>Practice Recommendations: Should address the specific authority that allows for the discretion to disclose/ re-disclose/mandate and discretion to evaluate/mandate to evaluate. Should cite specific statutes, executive orders, disclosure laws, paperwork reduction acts, etc. May also want to discuss ownership issues here (if not below).</p>
<p>7. Data to Be Shared</p> <p><Name of Lead IDS Agency> will provide access to the following data to <Data Licensee>:</p> <p>a. Integrated school, Medicaid, and human services data for all children aged 6-12 in the ____ School District from 2010-2016. All data are to be indexed (linked by unique dummy identifiers) at the individual student/person level.</p> <p>b. Etc.</p>	<p>Principles: Describe in detail the data that will be shared by the Lead IDS Agency, including structure of files, calculated variables, etc.</p> <p>Practice Recommendations: May wish to just broadly describe the data to be shared and then refer to a separate document or appendix that specifies the databases, elements/items, and formats, as well as other parameters such as geographic boundaries and dates ranges. May wish to provide a formal data dictionary for data licensee so that data parameters are clear.</p>

Example Text/Content of DUL Document	Comments*
<p>8. Ownership</p> <p>This DUL does not constitute a transfer of any title or interest in the Data, and <Name of Lead IDS Agency> reserves all rights in the Data not expressly granted to <Data Licensee> by this agreement. Any portion of the Data that is modified or merged into another form or merged with other Data shall continue to be subject to the provisions of this agreement.</p> <p><Name of Lead IDS Agency> makes no guarantee as to the accuracy or currency of the Confidential Information that will be provided as a result of this DUL.</p> <p>The person who will be the data custodian or control access to the data at <Data Licensee>, and will be responsible for ensuring the provisions of this agreement are carried out, is:</p> <p>Name</p> <p>Title</p> <p>Address</p> <p>Phone</p> <p>E-mail Address</p>	<p>Principles: Should set forth the ownership rights and responsibilities for the data that is subject to the DUL. Should also specify the custodian of the shared data (including contact information). This person should be personally responsible for carrying out the provisions of this agreement (including security controls, disclosure protocols, access protocols, etc.).</p> <p>Practice Recommendations: Address:</p> <ol style="list-style-type: none">Operational impact questions:<ol style="list-style-type: none">Who is responsible for veracity?Who is responsible for security?Who is responsible for updates?If there is a HIPAA violation, who is responsible?Structure of IDS and data extract may be important here.May want to consider copyright laws, intellectual freedom, and recent SCOTUS rulings around this. <p>May include disclaimer language such as: “Parties to this DUL do not make any representation or warranty, express or implied, as to the accuracy or completeness of any furnished information or other due diligence materials, and no Party, or any of its directors, trustees, officers, employees, shareholders, owners, affiliates, representatives, or agents, has or will have any liability to any other Party or person resulting from any reliance upon or use of, or otherwise with respect to, any furnished information or other due diligence materials.”</p>

Example Text/Content of DUL Document	Comments*
<p>9. Data Access Protocol</p> <p>Access to the requested data by <Data Licensee> will occur as follows:</p> <p><Data Licensee> will contact _____ at <Lead IDS Agency> to review protocols for securely logging in and accessing the requested data sets. Data are not to leave the secure servers of the <Lead IDS Agency> and all analyses will occur on such servers. . . .</p> <p>OR</p> <p><Lead IDS Agency> will coordinate the secure transfer of the requested data either through secure electronic protocols, or through exchange using appropriate physical media and following strong encryption procedures.</p>	<p>Principles: Describe the protocol for accessing and using the data extracts or data sets.</p> <p>Practice Recommendations: Describe process and security for direct access (VPN, remote login, etc.) or for data set transfer to Data Licensee. Use of graphics and schematics can help in the understanding of the protocols.</p> <p>This section may also address data security and confidentiality/privacy—if not covered separately below.</p>
<p>10. Roles and Responsibilities</p> <p>In accordance with the provisions of this agreement:</p> <p>A. The <Lead IDS Agency> will be responsible for:</p> <ol style="list-style-type: none">Compiling the shared data and facilitating access or transfer with <Data Licensee>Providing ongoing assistance in the use of the data and interpretation of findings/resultsEtc. <p>B. The <Data Licensee> will be responsible for:</p> <ol style="list-style-type: none">Securing and using the shared data according to provisions of this agreementInforming <Lead IDS Agency> of findings, dissemination of results, and disposition of the DataEtc.	<p>Principles: Clearly describe and delineate the agreed upon roles and responsibilities each organization or agency will be providing to ensure project success.</p> <p>Practice Recommendations: The roles and responsibilities should align with project goals, objectives, and target outputs.</p> <p>May want to include specific reference to the databases that will be used and the authorized studies that will be undertaken e.g., refer to the record layout. Some agreements have the record layouts in the appendix. Reference to specific studies may be better included in the Data Use and Permissions section below.</p>

Example Text/Content of DUL Document	Comments*
<p>11. Funding Information and Costs of Reimbursement</p> <p>This is a reciprocal data sharing agreement between <Lead IDS Agency> and <Data Licensee> and both parties acknowledge the benefit of the availability of integrated data via the <Lead IDS Agency> resource. As a result, neither party will charge the other party for the use of and access to data to be exchanged pursuant to this DUL, except as otherwise provided herein.</p> <p>OR</p> <p><Data Licensee> agrees to compensate <Lead IDS Agency> for the costs of compiling and providing access to the shared data. <Lead IDS Agency> will clarify such costs in a separate letter of engagement.</p> <p>OR</p> <p><Data Licensee> agrees to compensate <Lead IDS Agency> for the costs of compiling and providing access to the shared data. <Lead IDS Agency> will charge \$80 per hour for analyst time and \$5/GB per month for space on the <Lead IDS Agency> secure server. . . .</p>	<p>Principles:</p> <p><i>Funding:</i> If funds are to be obligated under the agreement, the financial arrangements to all parties must be clearly stipulated. If no funds are obligated under the agreement, a statement should be included that makes it clear that the agreement is not an instrument that obligates funds of any party to the agreement.</p> <p><i>Costs and reimbursement:</i> If the agreement result in the exchange of money between parties, state the estimated cost or costs not to exceed, terms of payments, and dispute resolution conditions.</p> <p>Practice Recommendations: May include differential pricing.</p>

Example Text/Content of DUL Document	Comments*
<p>12. Confidentiality and Privacy</p> <p>Parties understand that disclosure and re-disclosure of the Confidential Information is governed by both federal and state law. For example (and not by way of limitation), federal restrictions on this information are contained in 42 U.S.C. § 503, 26 U.S.C. § 3304, and subpart B of 20 C.F.R. Part 603, and the Family Educational Rights and Privacy Acts Statute (“FERPA”) against unauthorized access or re-disclosure. State law restrictions are contained in _____. Pursuant to these requirements, the parties (and each person having access to the data), covenant as follows, and agree that upon their receipt of any Confidential Information, they are representing that they have complied with and/or have accomplished, and will continue to comply with and accomplish, each of the following:</p> <p>1. Confidential Information will be used only for the purposes authorized by law and only for the purposes specified in this DUL;</p> <p>2. Access to Confidential Information will be provided only to authorized personnel who are required to perform activity required by this DUL and who need to access it for purposes listed in this DUL, who have executed a confidentiality certification. A signed copy of the Certification shall be provided by the individuals who sign this DUL;</p> <p>3. Parties will instruct all Authorized Personnel as to the confidential nature of all Confidential Information, the safeguards required to protect the information, the civil and any criminal sanctions for non-compliance pursuant to state laws.</p> <p>4. Parties and Authorized Personnel will strictly adhere to the requirements of this DUL and its required procedures, and will report any breaches fully and promptly;</p> <p>5. Parties will take precautions to ensure that only authorized personnel have access to the computer systems in which the Confidential Information is stored;</p> <p>6. Parties will implement safeguards and precautions to ensure that only Authorized Personnel have access to the Confidential Information;</p> <p>7. Parties will ensure that Confidential Information will be stored in a place physically secure from access by unauthorized persons;</p> <p>8. Parties will ensure that Confidential Information in electronic format is stored and processed in such a way that unauthorized persons cannot retrieve the information by means of computer or otherwise gain access to it;</p> <p>9. Parties shall immediately terminate an individual’s authorized access upon changes in the individual’s job duties that no longer require access, unauthorized access to, or use of Confidential Information by the individual, or termination of employment; and</p> <p>10. Parties shall transmit the Confidential Information by a secure method and encrypt all personally identifiable information (PII) during receipt, transmission, storage, maintenance, and use.</p>	<p>Principles: Address how privacy will be ensured and how confidential information will be protected (if not addressed above in data description).</p> <p>Practice Recommendations:</p> <p>Confidentiality, privacy, and data security are all separate issues.</p> <p>1. <i>Confidentiality</i> refers to that which is done in confidence with the expectation of privacy</p> <p>2. <i>Privacy</i> means the right to restrict access to private information</p> <p>3. <i>Data security</i> is separate section</p> <p>Should identify the relevant statutes on confidentiality. Discuss issues of training, access, and storage and who is responsible for training, access, and storage. Discuss how to address state law and how to deal with pre-emption. May want to require compliance with any oversight boards (e.g., IRB) and stipulate that individuals who are approved to work on joint projects to be trained on safeguard to protect confidential information.</p> <p>Reference relevant statutes: e.g., HIPAA; FERPA; The Common Rule Privacy Act of 1974; 42 CFR; HMIS Children’s Online Privacy Act; Child Abuse Prevention and Treatment Act</p>

Example Text/Content of DUL Document	Comments*
<p>13. Data Security</p> <p><Data Licensee> will use appropriate safeguards to prevent use or disclosure of the individually identifiable information other than as provided for by this Agreement. <Data Licensee> will maintain and use appropriate administrative, technical, and physical safeguards to preserve the integrity and confidentiality of the IDS and to prevent non-permitted use or disclosure of individually identifiable information.</p> <p><Lead IDS Agency> will ensure that any agent, including a subcontractor, to whom it provides individually identifiable information, received from, or created or received by <Lead IDS Agency>, executes a written agreement obligating the agent or subcontractor to comply with all the terms of the Agreement.</p>	<p>Principles: Includes policies and procedures to protect the confidentiality and safety of data.</p> <p>Practice Recommendations: Discuss:</p> <ol style="list-style-type: none">1. who is responsible for data security;2. who is responsible for keeping data-use agreements; what records should be retained; back-up systems; the duration of time that records should be retained;3. specific protocols for physical and virtual/electronic security— be specific about proposed security arrangements and demonstrate full understanding of applicable statutes, regulations, and traditional practices;4. how data security changes with industry standards (consider resources such as the SANS Institute [sans.org] and CERT at Carnegie Mellon University [cert.org]);5. how parties can inspect security arrangements for the purpose of confirming the user is in compliance with data security procedures and requirements specified by the agreement.

Example Text/Content of DUL Document	Comments*
<p>14. Data Use, Permissions, and Retention</p> <p>A. Data will be transferred to/accessed by <Data Licensee> using the following secure protocols outlined in Section 9 above.</p> <p>B. If applicable, permissions and consents to use the data will be provided by the <Lead IDS Agency> to comply with any applicable state or federal laws and/or regulations.</p> <p>C. <Data Licensee> will not disclose or re-disclose any shared or accessed data with any other entities or persons without explicit written permission of <Lead IDS Agency>.</p> <p>D. <Data Licensee> will not use or disclose individually identifiable information other than as permitted or required by this Agreement, or as required by state and federal law, or as otherwise authorized by data owners.</p> <p>E. <Data Licensee> agrees <u>not</u> to perform any of the following actions:</p> <ol style="list-style-type: none">a. Attempting to identify any individual whose health information is included in a de-identified Limited Data Set.b. Using or further disclosing any data for any purpose other than the purpose specified above or as otherwise permitted by law.c. Publishing or otherwise disclosing information that identifies the individuals whose health information is included in shared data. <p>F. <Data Licensee> agrees not to use or permit others to use shared data that identify an entity or individual health care provider for any of the following purposes:</p> <ol style="list-style-type: none">a. To compete commercially against an entity.b. To determine the rights, benefits, or privileges of an entity or individual health care provider.c. To report, through any medium, information that identifies an entity or individual health care provider. <p>G. <Data Licensee> will use appropriate safeguards to prevent use or disclosure of the individually identifiable information other than as provided for by this Agreement. <Data Licensee> will develop, implement, maintain, and/or use appropriate administrative, technical, and physical safeguards to preserve the integrity and confidentiality of and to prevent non-permitted use or disclosure of individually identifiable information (see section 13 above). These safeguards are required regardless of the mechanism used to transmit the information. <Data Licensee> will document and keep these safeguards current.</p> <p>H. Shared data will be retained by <Data Licensee> for the duration of this agreement and any renewals of this agreement. Back-up systems will be implemented according to industry standards to appropriately secure the back-up media/files. Upon termination of this agreement, shared data and back-up files will be permanently deleted (e.g., using overwrite protocols) within 80 days of the termination date. <Data Licensee> is responsible for providing confirmation of such data destruction.</p>	<p>Principles: Define the scope and process of using data, as well as data transfer protocols.</p> <p>Practice Recommendations:</p> <p>Describe issues such as:</p> <ol style="list-style-type: none">1. How the data will be securely transferred or accessed.2. Record usage, duplication, and re-disclosure restrictions: limitations on the access to, disclosure, and use of information. Who can access the data? Limitations on identifiable data? Where can research/analysis be done?3. Use of administrative data for other projects: specify the project and/or uses for which the other agency can use the administrative records described by the DUL.4. Data available for researchers: Consider whether the data subject to these administrative records will be made available to researchers or to the public. Are restricted data use licenses implicated? What kind of public disclosures need to be made?5. Describe any required statutory firewalls.6. Data retention—including what records shall be retained for the project contemplated by the agreement and for a back-up system. Specify the duration of time that records should be retained.

Example Text/Content of DUL Document	Comments*
<p>15. Notification of results, dissemination of results, and dissemination of end products</p> <p><Data Licensee> will notify and provide draft copies of results and findings derived from analyses of contributed data produced by <Data Licensee>, its employees, subcontractors, or other Authorized Personnel. Such results and end products must be provided to the <Lead IDS Agency> no less than 45 days prior to the dissemination of such results or products. Such notice should be provided to the following individuals at <Lead IDS Agency>:</p> <p>Name Title Address Phone E-mail Address</p> <p>Alternate Contact:</p> <p>Name Title Address Phone E-mail Address</p> <p><Lead IDS Agency> and original data owners will then have 45 days to offer relevant review for accuracy, appropriate citations, etc., and acknowledgment of the results or products. <Data Licensee> may presume acknowledgment if none is forthcoming within the 45-day review period.</p>	<p>Principles: Describe protocols for providing notice of dissemination of findings from data analyses.</p> <p>Practice Recommendations: If the parties are releasing any documents or research related to the exchange of administrative data, specify the subject matter, rights, and responsibilities pertaining to the public use of data. Data citations should also be discussed here as well as definitions for documenting data linking and cleaning process.</p> <p>May also wish to include provisions for an evaluation of the Data Licensee process and use of the shared data, if desired.</p>
<p>16. Term of Agreement</p> <p>This DUL will be effective on the date that the last Party has executed it (the “Effective Date”), and shall terminate on the date that is ____ years from the Effective Date, unless such term is extended by mutual agreement. This term of agreement is subject to the termination provisions in section 24 below.</p>	<p>Principles: State specific start and end dates of DUL.</p> <p>Practice Recommendations: If the completion date is not known and the period of the agreement is expected to stretch over a number of years, the completion date may be listed as indefinite.</p>

Example Text/Content of DUL Document	Comments*
<p>17. Performance Standards and Review Procedures</p> <p><Data Licensee> understands that <Lead IDS Agency> and other statutory authorities have the right to audit <Data Licensee>’s policies, procedures, and implementation of those policies and procedures for safeguarding the shared data and preserving the confidentiality of information. In addition, <Lead IDS Agency> shall be permitted to audit and monitor <Data Licensee>’s and its employees’ access to and use of the Confidential Information on a periodic and “as needed” basis, including on-site inspections, to determine compliance with this DUL. <Data Licensee> agrees to cooperate fully with any auditing or on-site inspections. All reasonable costs of the auditing authority for such auditing and inspection shall be the sole expense of <Lead IDS Agency>. <Data Licensee> shall create and maintain a system sufficient to allow an audit of compliance with the requirements of this DUL.</p>	<p>Principles: If the agreement is extended for an indefinite period of time, it should contain a provision for review at least every three years to determine the continuing need and whether the agreement should be revised, renewed, or cancelled.</p> <p>Practice Recommendations: Should include provisions for audits:</p> <p>1. Should specify who is responsible for audit</p> <p>2. Should specify the components of the audit report (citing strengths, deficiencies, and any corrective actions that need to be taken).</p>
<p>18. Resolution of Conflicts</p> <p>In the event a party to the DUL believes that a provision of the DUL has been breached, or if there is a disagreement regarding implementation of the DUL or any of its provisions, the parties agree to attempt to resolve the conflict in the following manner:</p>	<p>Principles: Set forth the method for settling disputes short of termination of agreement.</p> <p>Practice Recommendations: Steps may include:</p> <p>1. Notice of dispute and good faith attempt to resolve through negotiation</p> <p>2. Mediation</p> <p>3. Arbitration</p>

Example Text/Content of DUL Document	Comments*
<p>19. Unauthorized disclosure of information or other breach</p> <p><Data Licensee> will report to <Lead IDS Agency>, in writing, any use and/or disclosure of individually identifiable information that is not permitted or required by this Agreement of which <Data Licensee> becomes aware. Such report shall be made as soon as reasonably possible but in no event more than ten (10) business days after discovery by <Data Licensee> of such unauthorized use or disclosure. This reporting obligation shall include breaches by <Data Licensee>, its employees, subcontractors, agents, or Data Licensees. Each such report of a breach will:</p> <p>a. identify the nature of the non-permitted use or disclosure;</p> <p>b. identify the individually identifiable information used or disclosed;</p> <p>c. identify who made the non-permitted use or disclosure;</p> <p>d. identify who received the non-permitted use or disclosure;</p> <p>e. identify what corrective action <Data Licensee> took or will take to prevent further non-permitted uses or disclosures;</p> <p>f. identify what <Data Licensee> did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and</p> <p>g. provide such other information as <Lead IDS Agency>, or the data owners, may reasonably request.</p> <p><Add indemnification and/or liquidated damages language></p>	<p>Principles: Specify the remedies and damages in the event of a breach of contract by any party to the agreement or unauthorized disclosure of data.</p> <p>Practice Recommendations: Describe:</p> <p>1. the responsibilities for notification by points of contact of each party to the DUL.</p> <p>2. any criminal/civil penalties that may apply for unauthorized disclosure of information.</p> <p>3. indemnification language and limitations of liability.</p> <p>4. any liquidated damages for breach of agreement if applicable.</p> <p>May want to specify Parties negotiating an agreement often make an explicit agreement as to what each party's remedy for breach of contract shall be.</p>
<p>20. Supersedes</p> <p>This DUL <u>supersedes</u> any previous understandings, representations or agreements, whether written or oral, that may have been made or entered into by the parties relating to the subject matter hereof.</p> <p>OR</p> <p>This DUL does <u>not supersede</u>, replace or render invalid any other agreement. . . . The Participants mutually agree to promote and advance the purpose of this DUL to enhance information sharing, when necessary, beyond any existing understandings or agreements, including this one.</p>	<p>Principles: Establish relationship of this agreement with other understandings or agreements between the parties.</p>
<p>21. Severability</p> <p>Nothing in this DUL is intended to conflict with the current laws, regulations, or policies applicable to each Party. If a term of this DUL is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this DUL shall remain in full force and effect.</p>	<p>Principles: Establish severability of terms of the DUL.</p>

Example Text/Content of DUL Document	Comments*
<p>22. No Private Right of Action</p> <p>This agreement does not create any private cause of action for enforcement or damages.</p>	<p>Principles: Clarify that the DUL does not create a private right of action.</p>
<p>23. Modification/Amendment of the DUL</p> <p>Modifications or Amendments to this DUL must be in writing and formally agreed to/executed by all Parties. Concurrence provisions below apply.</p> <p>OR</p> <p>There shall be no modifications or amendments of this DUL, except in writing, executed with the same formalities as this instrument.</p>	<p>Principles: Set forth the process for amending the DUL.</p> <p>Practice Recommendations: Amendments should be with consent of all parties to the DUL and in writing.</p>
<p>24. Termination of the DUL</p> <p>Either party may, with or without cause, terminate this DUL by giving an eighty (80) day written notice of its intent to do so. In the event changes in either state or federal law or regulations occur which render performance hereunder illegal, void, impracticable, or impossible, this DUL shall terminate immediately; However, obligations with respect to the treatment and security of Confidential Information and shall survive any termination of this DUL.</p>	<p>Principles: Set forth process for termination of the DUL.</p> <p>Practice Recommendations: Should contain a provision whereby each party may terminate the agreement with a specified time frame. Note: The MOU template between original data owners and Lead IDS Agency have a 90-day termination notice requirement; thus if original data owners provide such termination notice, the Lead IDS Agency should promptly (within 10 days) give all Data Licensees using the data their 80-day notice of termination.</p>
<p>25. Concurrence</p>	<p>Principles: In order to be a valid agreement, there must be concurrence by all parties to the agreement.</p> <p>Practice Recommendations: Identify the agency signatories. Agency signatories agree that they have the authority to sign for the agency or participating entity and denote their acceptance of the agreement terms by affixing their signature and the date.</p>

Allegheny County – School Districts

MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding ("MOU") is entered into by and between The _____ School District (the "District"), with an address of _____ and Allegheny County Department of Human Services ("DHS"), with an address of 1 Smithfield Street, Pittsburgh, PA 15222.

WHEREAS, the School District wants to identify attributes and indicators for academic and behavioral successes or challenges, and

WHEREAS, identifying these attributes and indicators will enable the District and DHS to create and implement strategies and/or interventions to improve student aid programs and ultimately improve instruction and student performance, and

WHEREAS, a Blue Ribbon Commission identified Allegheny County Department of Human Services as an organization that is willing and able to conduct research on behalf of the District, and

WHEREAS, DHS has the capabilities to integrate student-level data with existing DHS data and identify attributes and indicators for academic and behavioral successes or challenges, and

WHEREAS, DHS has offered to perform services and carry out activities which, pursuant to the undertakings and terms of this MOU, qualifies it as an organization that conducts studies for, or on behalf of educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, or improving instruction; and

WHEREAS, DHS will require access to educational records and/or personally identifiable information for the purpose of completing the services and research required by this MOU; and

WHEREAS, the School District requires this MOU including specific confidentiality provisions prior to the release of any educational records or personally identifiable information contained therein in accordance with the Family Educational Rights and Privacy Act (FERPA), 20 USC 1232g, and its implementing regulations at 34 CFR Part 99, as amended.

NOW, THEREFORE, with the intent to be legally bound hereby, the parties to this MOU set forth the following as the terms and conditions of their understanding.

The District and DHS hereby agree as follows:

1. **Background.** The Allegheny County Department of Human Services (DHS) is responsible for providing and administering human services to county residents. DHS is dedicated to meeting these human services needs, most particularly to the county's most vulnerable populations, through an extensive range of prevention, early intervention, crisis management and after-care services provided through its program offices.

DHS services include: Programs serving the elderly, mental health services (includes 24-hour crisis counseling); drug and alcohol services; child protective services; at-risk child development and education; hunger services; emergency shelters and housing for the homeless; energy assistance; non-emergency medical transportation; job training and placement for youth and adults; and services for individuals with mental retardation and developmental disabilities.

The Allegheny County Department of Human Services serves approximately 230,000 people in Allegheny County per year. The population in the School District of

DHS and the District believe that sharing certain student data could be beneficial to the students and improve the services and student aid programs provided to students by both parties. DHS has agreed to conduct an action research study to identify attributes and indicators for academic and behavioral successes and challenges. The parties will examine the findings and reports issued by DHS during the term of this MOU, develop strategies utilizing the findings, and determining the benefit of that information and its effect on the administration of student aid programs and improving instruction.

This project acknowledges that both the District and DHS can better instruct and otherwise serve children and their families by sharing information. The goal is to inform operational issues with which both Parties struggle and to improve instruction while also improving aid and services available to the students.

2. **Term.** The term of this MOU shall commence on the date it is approved or ratified by the District's Board of Directors (the "Effective Date") and shall expire three calendar years afterwards on _____. The term may be extended by written mutual consent of the parties which written consent includes a scope of work referencing this MOU and setting forth the responsibilities of the parties.
3. **Scope of Work.**

3.1 **Responsibilities of DHS.**

- 3.1.1. **DHS as Legal Custodian.** DHS agrees to provide the District with identifying information for all students for whom Allegheny County serves as legal custodian and to participate in the education of those children as an active parent or guardian.

For the purposes of this agreement, Legal Custody refers to all students who are either placed pursuant to a court order or identified as adjudicated dependent in the Common Pleas Court Management System (CPCMS).

Identifying information includes Personal Identifiers (first name, last name, date of birth, gender, race, home address) and contact information for the student's primary Child Welfare Caseworker (first name, last name, phone number, email address, regional office, supervisor).

3.1.2 DHS serving Homeless Children

DHS agrees to provide the District with identifying information (first name, last name, date of birth, gender, race, home address) for all students who are identified as homeless by DHS using the HUD definition of homeless. Providing this data will assist students receive school supports as stated in the McKinney-Vento Homeless Assistance Act.

3.1.3 Action Research.

Statistical Analysis. DHS agrees to integrate student data into its existing data warehouse and generate analytical reports that provide the distributions of students receiving DHS services across the District. The analytical reports shall be de-identified aggregate reports. DHS shall identify attributes and indicators for academic and behavioral successes and challenges.

Critical Reflection. DHS shall present the analysis to all parties and together engage in careful examination of the data in an effort to develop effective strategies for improving both organizations' ways of working with children and families.

Action. DHS shall create, implement, and assess strategies developed through the statistical analysis and critical reflection phases. DHS shall work with the District to implement these strategies in schools and in the community.

3.1.4 Consent for Release of Records. DHS agrees to request parental consent from students receiving DHS services when the parties determine that additional intervention is needed and the student would benefit from direct collaboration between DHS and the District. The following release shall be requested:

- Consent for the School District to release education records to DHS; and
- Consent for DHS to release service data to the School District.

3.2 **Responsibilities of District.** In support of this initiative, the District agrees to:

3.2.1 Provide DHS with access to all directory information and education records for those students whom DHS is the legal custodian.

3.2.2 The District agrees to provide the following information for students enrolled in the School District:

- Personal Identifiers – first name, last name, date of birth, gender, race, home address, social security number, school and grade level

- Achievement – grade point average (if calculated), progress reports if indicating a failing grade
- Attendance – excused/unexcused absences, truancy filings, withdrawals and/or dropout
- Specialized Programming – Student Assistance Program, Special Education status (identified or not identified as a student receiving special education and related services or identified as receiving Gifted Education)
- Additional information as agreed upon by the parties.

3.2.3 The District shall provide directory information for all school age students residing in the District.

3.2.4 Action Research.

Critical Reflection. The District shall participate in the critical reflection phase of this action research project and work to identify strategies and interventions to improve student aid programs based on the information provided by DHS.

Action. The District shall create, implement, and work with DHS to assess strategies and interventions to improve student aid programs and improve instruction.

3.3 **Confidentiality.**

3.3.1 All student data provided by the District is considered to be confidential under this MOU as well as under the Family Educational Rights and Privacy Act (FERPA), 20 USC §1232g. *et seq.*, and any other federal or state statutes or regulations pertaining to student records, and will only be released in accordance with the applicable laws and regulations.

3.3.2 All reports containing personally identifiable information generated as a result of this study shall also be confidential and shall not be released without the mutual consent of the parties unless otherwise required by law.

3.3.3 The parties hereby acknowledge and agree that any confidential documents and/or data provided by the District or by DHS, shall not be disclosed, discussed or transferred to any third party not party to this MOU, and any student data or information provided to DHS shall only be disclosed to employees of DHS and District employees who are directly involved in the data integration study, or to other parties so long as no personally identifiable information is discernible. DHS agrees to execute any additional confidentiality agreement to enable implementation of this MOU.

- 3.3.4 Upon the expiration of this MOU, all student data and information that is not otherwise the legal property of DHS shall be either returned to the District or destroyed. DHS shall provide written verification that all copies of student data, information and documents, including electronic or other media versions, have been returned to the District or destroyed. DHS shall, however, be allowed to continue to possess aggregate numbers and statistics created based on student data which is used to measure the effectiveness of the data integration study.
- 3.3.5 DHS understands and agrees that should the District find that DHS has violated Section 3.3 or any of the applicable laws and regulations regarding confidentiality of student records, the District shall be entitled to immediately cease providing data for the program and shall be prohibited from permitting DHS access to information from education records for a period of not less than five (5) years.
- 3.3.6 District understands that DHS may need to conduct both qualitative and quantitative research to determine the effectiveness of its programs. Qualitative data could include surveys, interviews, and focus groups with teachers, administrators, students, and/or parents. DHS agrees that all requests to conduct qualitative and quantitative research within the District shall be in accordance with the Protection of Pupil Rights Act (PPRA) (20 U.S.C. §1232h; 34 CFR Part 98) and the District's Internal Review Board (IRB) policy and administrative regulations. The District commits not to withhold permission for such additional research unreasonably and to create a streamlined process to expedite approval of such requests.
- 3.4 **Clearances.** DHS staff and DHS contractors that will have direct contact with students shall obtain and submit all clearances required by 24 P.S. §1-111 and 23 Pa.C.S. §§6354 *et seq.*
- 3.5 **District Contact.** Communications from DHS will be coordinated initially with [REDACTED].
4. **Community Stakeholders.** The parties agree to engage community stakeholders in the action phases of this research project. No confidential data will be released or discussed with third parties, but the parties may agree to disclose de-identified aggregate reports to support their initiatives and engage community stakeholders.
5. **Costs.** This joint venture shall not result in the transferring of funds from one entity to another. However, DHS agrees to provide technical assistance to the District to develop and effect the initial data extract. If the parties determine that additional staff or supports are necessary at any stage of this research project, DHS agrees to seek funding to support those needs.

6. **Intellectual Property.**

- 6.1 **Copyright.** The District reserves copyright in all written and electronic materials developed by the District or District employees as a part of their employment with the District. District materials may not be copied or otherwise reproduced without the express written permission of the District. DHS reserves copyright in all written and electronic materials delivered and developed by DHS pursuant to this MOU, including materials developed by DHS with input from District staff.
- 6.2 **Trademark and Trade Name.** This MOU does not give DHS any ownership rights or interest in District trade names or trademarks. This MOU does not give the District any ownership rights or interest in DHS trade name or trademarks.
- 6.3 **Use of Name.** DHS shall obtain the District's consent prior to using the District's name in any report or publication.

7. **Evaluations.** The District reserves the right to evaluate the effectiveness of this MOU and the information provided by DHS as needed throughout the term of this MOU.

8. **Independent Contractors.** During the performance of this MOU, the employees of one party will not be considered employees of the other party within the meaning of any federal, state or local laws or regulations including, but not limited to, laws or regulations covering unemployment insurance, old age benefits, workers compensation, industrial accident, labor or taxes of any kind nor within the meaning or application of the other party's employee fringe benefit programs for purposes of vacations, holidays, pension, group life insurance, accidental death, medical, hospitalization and surgical benefits. The District's employees who perform the obligations of the District hereunder shall be under the employment and ultimate control, management and supervision of District. DHS' employees or contractors who are to perform the services to be completed by DHS hereunder shall be under the employment and ultimate control, management and supervision of DHS. Nothing contained herein shall be construed to imply a joint venture, partnership or principal-agent relationship between the District and DHS, and neither party shall have the right, power or authority to obligate or bind the other in any manner whatsoever, except as otherwise agreed to in writing.

9. **Termination.** This MOU may be terminated by either party upon ninety (90) days written notice to the addresses set forth in Section 13.

10. **Entire Understanding.** This MOU constitutes the entire and sole understanding between the parties with respect to the subject matter hereof and supersedes any prior written agreements and any prior, contemporaneous or subsequent oral understanding, with respect to the subject matter hereof.

11. **Modification or Amendment.** There shall be no modifications or amendments of this MOU, except in writing, executed with the same formalities as this instrument.

12. **Conflict.** In the event of any conflict, ambiguity or inconsistency between this MOU and any other document which may be annexed hereto, the terms of this MOU shall govern.
13. **Notices.** Any notices and other communications provided hereunder shall be made or given hereunder by either party by facsimile or email as set forth below or delivered by hand or by mail to the party at the address set forth below:

FOR THE [REDACTED] SCHOOL DISTRICT:

Superintendent:

Address:

Phone:

Email:

Solicitor

Phone:

Fax:

Email:

FOR DHS:

Marc Cherna

Allegheny County

Department of Human Services

1 Smithfield Street

Pittsburgh, PA 15222

Phone: 412-350-5705

Fax: 412-350-4004

Email: marc.cherna@alleghenycounty.us

14. **Limitations on Liability.** In no event shall either party be liable to the other party under this MOU or to any third party for special, consequential, incidental, punitive or indirect damages, irrespective of whether such claims for damages are founded in contract, tort, warranty, operation of law, or otherwise, or whether claims for such liability arise out of the performance or non-performance by such party hereunder.
15. **Governing Law.** This MOU shall be construed to be made and interpreted under the laws of the Commonwealth of Pennsylvania and all disputes, claims or controversies arising under this MOU or the negotiations, validity or performance hereof for the transaction contemplated herein shall be construed under and governed by the laws of the Commonwealth of Pennsylvania without giving effect to conflicts of law principles which would result in the application of the laws of any other jurisdiction.
17. **Severability.** If any portion of this MOU is to be void, invalid, or otherwise unenforceable, in whole or part, the remaining portions of this MOU shall remain in effect.

18. **Headings.** The article and section headings in this MOU are for convenience of reference only and in no way define or limit the scope or content of the MOU or in any way effect its provisions.

IN WITNESS WHEREOF, the parties hereto set their hand(s) and seal(s) this ____ day of _____, 20____.

ATTEST:

**ALLEGHENY COUNTY
DEPARTMENT OF HUMAN SERVICES**

Witness

By:_____
Marc Cherna, Director of the Department of
Human Services

William McKain, County Manager

Approved as to Form Only:

By:_____

ATTEST:

SCHOOL DISTRICT OF

Secretary

By:_____
Board President

Approved as to Form Only:

Date of Board Approval:_____

By:_____
Solicitor

District of Columbia Public Schools (DCPS) Confidentiality Provisions

Appendix IV: Key Provisions from the DCPS Confidentiality Agreement

Researcher agrees to fulfill their responsibility on this project in accordance with the following guidelines:

1. To comply in all respects with the provisions outlined in (a) the DCPS Process and Requirements to Conduct Research or Obtain Confidential Data, and (b) the MOA between my organization and/or myself and DCPS.
2. To comply in all respects with applicable provisions of the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).
3. To maintain, use, disclose, and share data received pursuant to the MOA in a manner authorized by FERPA and any applicable federal and District of Columbia law or regulation.
4. To use data shared under the MOA with DCPS for no purpose other than the research project described in the MOA, and as authorized under 34 CFR §§ 99.31(a)(6). Nothing in the MOA shall be construed to authorize me/my organization to have access to DCPS data beyond that included in the scope of the MOA. I/my organization further agree not to share Confidential Data received under the MOA with or permit access to such data by any individual or entity other than the Parties named in the MOA, for any purpose, except as permitted by the MOA and applicable law. I/my organization shall put procedures in place to safeguard the confidentiality and integrity of Confidential Data, to place limitations on its use and to maintain compliance with applicable privacy laws. I understand that the MOA does not convey me/my organization ownership of any Confidential Data.
5. To obtain all necessary approvals from authorized officials of my organization prior to beginning the Project. I will also obtain informed consent from Project participants as described in the DCPS Process and Requirements to Conduct Research or Obtain Confidential Data.
6. To require all employees, contractors, and agents of any kind working on the research project described in the MOA to comply with the MOA, the DCPS Process and Requirements to Conduct Research or Obtain Confidential Data, and all applicable provisions of FERPA and other laws with respect to the data and information shared under the MOA. I agree to require each employee, contractor, or agent with access to data to sign a security pledge and to provide such signed security pledges to DCPS.
7. To the extent DCPS has not provided student records with Personally Identifiable Information, I agree not to attempt to identify individuals, families, or households in such data except as required by the project described in the MOA. I shall not disclose data produced to me/my organization under the MOA in any manner that could identify any individual or school, except as authorized by FERPA, to any unauthorized person. I and persons participating in this project on behalf of the Parties named in the MOA shall neither disclose nor otherwise release data and reports relating to an individual or school, nor disclose information relating to a group or category of individuals without ensuring the confidentiality of individuals in that group. Publications and reports of these data and information related to them, including preliminary project descriptions and draft reports,

shall involve only aggregate data and no personally identifiable information or other information that could lead to the identification of any individual or school.

8. To not publish nor report on any DCPS data or information without first obtaining express written permission from DCPS.
9. To not provide any Confidential Data obtained under the MOA to any entity or person ineligible to receive Confidential Data or prohibited from receiving Confidential Data by virtue of a finding under 34 CFR § 99.31(a)(6)(iv), in any form, including electronically (including email) and hard copy.
10. To not share any Confidential Data obtained under the MOA via email with any entity or person including others participating in the project described in the MOA.
11. To notify DCPS immediately in the event of a breach of any measures to keep confidential the data received pursuant to my/my organization's MOA with DCPS. I will also make all reasonable efforts to cure any such breach and to prevent further breaches, and to inform DCPS of such efforts.
12. To destroy all Confidential Data as provided for in the MOA.

State of California Global Memorandum of Understanding – Child Welfare Services

If requested, return material to:
Contracts and Purchasing Bureau
M.S. 8-14-747

GEN 944 (05/08)

GLOBAL MEMORANDUM OF UNDERSTANDING CHILD WELFARE SERVICES

I. RECITALS

This Memorandum of Understanding (MOU) is entered into by and between the California Department of Social Services (CDSS), the California Department of Health Care Services (DHCS), and those California Counties and Title IV-E Tribes that have agreed to the terms and conditions of this MOU by becoming signatories to this MOU (hereafter "parties"); to set forth the terms and conditions for the exchange of confidential data, collected and retained by CDSS and DHCS (Department(s)), for the purpose of matching the confidential data, hereinafter referred to as 'matched data,' to administer and implement the applicable federal and/or state health and public social service programs described herein. This MOU also sets forth the terms and conditions imposed on each Department, when it is necessary for program purposes, to share identifiable and de-identified matched data with signatory California counties and Title IV-E Tribes (hereafter "counties or tribes"), authorized entities and de-identified data with the public.

CDSS and DHCS, pursuant to Welfare and Institutions Code (WIC), Division 9, § 10000 *et seq.*, are responsible for the administration and delivery of public social services.

WIC § 10051 defines 'public social services' as:

"...activities and functions of state and local government administered or supervised by the department or the State Department of Health Services and involved in providing aid or services or both, including health care services and medical assistance, to those people of the state who, because of their economic circumstances or social conditions, are in need thereof and may benefit thereby."

Specifically, CDSS is the single state agency under Title IV of the Social Security Act that is responsible for oversight of county and community agencies in the implementation of child welfare services programs which includes services for children in foster care and other services provided on behalf of children who are or are alleged to be the victims of child abuse, neglect, or exploitation. CDSS responsibilities include, but are not limited to, implementing the state Health Care Oversight Plan under Title IV-B and IV-E to ensure that the physical and mental health needs of children in foster care are identified and met. Pursuant to WIC § 10850, CDSS is authorized to provide confidential data to county public agencies, private agencies, and Native American tribes with a Title IV-E agreement pursuant to WIC § 10553.1 (hereinafter Title IV-E tribe) that are directly connected with the administration of these programs by providing, or securing, public social services, for or on behalf of applicants or recipients.

Specifically, DHCS is the single state agency under Title XIX of the Social Security Act that is responsible for operating and overseeing the federal Medicaid program in California, hereafter referred to as Medi-Cal. DHCS responsibilities, include, but are not limited to, ensuring high-quality and efficient health care services are provided to Medi-Cal beneficiaries, which categorically include children in foster care and former foster youth who attain age 18 while in a foster care placement. Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), DHCS is authorized to provide and exchange protected health information (PHI) of an individual for the purposes of treatment, payment, and health care operations (See 45 CFR § 164.502). Health care operations includes: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance

activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities (See 45 CFR§ 164.501).

Specifically, pursuant to WIC §10800, the counties are responsible for the administration and provision of public social services, including child welfare services, in each county of the state. The provision of public social services in the counties must comply with state and federal laws including the regulations of the CDSS and DHCS. Further, Title IV-E tribes, through their agreements with either the State or directly with the federal government, are responsible for ensuring the health and safety of children or non-minor dependents receiving child welfare services under the jurisdiction of the tribe.

Based on the federal and state authority of each Department, the obligation of the counties and Title IV-E tribes to administer public social services, and for the purpose of complying with each Department's respective and mutual responsibilities and requirements as it pertains to children or non-minor dependents receiving child welfare services and former foster youth, the parties hereby agree to the following terms and conditions in the exchange of confidential data and use of matched confidential data.

II. PURPOSE

The parties agree to the exchange of both confidential and non-confidential data. The use and disclosure of such data shall be limited to the following purposes:

1. Analysis and reporting for the purposes set forth in 42 USC § 622(b)(15) which includes, but is not limited to:
 - a) Ongoing oversight of health care services for any children or non-minor dependents receiving child welfare services;
 - b) Ensuring a coordinated strategy to identify and respond to the health care needs of children or non-minor dependents receiving child welfare services; and
 - c) Ensuring Medi-Cal enrollment for former foster youth up to age 26 and, through data sharing, facilitating the extension of Medi-Cal enrollment of existing foster care youth up to age 26 as they exit the program.
2. Analysis, reporting, and auditing to provide ongoing administration, operation oversight, coordination, program monitoring, and evaluation of health treatment, including mental health services and pharmaceutical services to children or non-minor dependents receiving child welfare services.
3. Reporting federal Adoption and Foster Care Analysis and Reporting System (AFCARS) data elements as described per § 479 of the Social Security Act and 45 CFR § 1355.
4. To share amongst the parties, as applicable and appropriate, matched data containing confidential information and de-identified data, reports and analyses based upon matched data to support the administration and provision of public social services to children or non-minor dependents receiving child welfare services.

III. DEFINITIONS

“Breach” shall have the meaning given to such term under HIPAA and the HIPAA regulations and includes any known or suspected information security incidents (intentional or unintentional, that cause or may cause loss, damage, destruction, misuse, or unauthorized disclosure of information, as provided in the Social Security Administration Information Exchange Agreement (SSA IEA)); the CDSS Confidentiality and Security Requirements for California State Agencies; and the California Information Practices Act.

“Children or non-minor dependents receiving child welfare services” means children or non-minor dependents on whose behalf the county child welfare agency or probation department is providing child welfare services as described in WIC § 16501(a). This includes, but is not limited to, the following:

1. Children and non-minor dependents who are dependents of the juvenile court or are receiving voluntary child welfare services.
2. Children and non-minor dependents who are wards of the juvenile court and are in a foster care placement.
3. Children and non-minor dependents who are receiving child welfare services provided by a tribe with a Title IV-E agreement.

“Confidential data” means Information that identifies or is substantially likely to identify an individual and that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or has restrictions on disclosure in accordance with other applicable state or federal laws, including but not limited to WIC 10850. As used in this MOU Confidential data may include Protected Health Information (PHI), or Individually Identifiable Health Information as defined in HIPAA, 45 CFR 160.103; or “Limited data set (LDS)” as defined in 45 CFR 164.514; or Personal Information (PI), as defined in California Civil Code, §§ 1798.3, 1798.24 and 1798.29; or Personally Identifiable Information (PII), as defined in the Social Security Administration Information Exchange Agreement (SSA IEA) and DHCS Business Associate Addendum (BAA).

“Counties” means the largest political subdivision of the State having corporate powers (Govt. Code section 23000). As used in this MOU counties refers to the current 58 counties of California.

“Data” is a representation of facts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automated means. As used in this MOU data would refer to information related to children receiving child welfare services or non-minor dependents or former foster youth.

“Alcohol and Drug Abuse Patient Records data” covered by 42 CFR Part 2, is excluded from this MOU.

“De-identified data” means information that does not identify an individual such that there is no reasonable basis to believe that the information provided can be used to identify an individual. HIPAA provides that data can be considered de-identified if a person experienced in statistical methods for rendering information not identifiable determines the risk is small that the information could be used to identify an individual or specific identifiers identified in the HIPAA regulations are removed (45 CFR 164.514(a) and (b)(1) or (b)(2)). De-identified data is not PHI.

“Department(s)” means the California Department of Social Services and/or the California Department of Health Care Services.

“Former Foster Youth” means a former non-minor dependent, as defined by WIC § 11400(v), who was in foster care on his or her 18th birthday and is under the age of 26 at the time of any request for data, regardless of whether the youth is receiving any child welfare service.

“Matched data” means the combining of confidential health and child welfare services information from a covered entity to a business associate for analyses and use that relates to the health care and child welfare services operations of the respective entities (also known as data aggregation under 45 CFR 164.501).

“Personal Information” (PI) means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.” (CA Civil Code section 1798.3)

“Personally Identifiable Information” (PII) is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. An item such as date and place of birth, mother's maiden name, or father's surname is PII, regardless of whether combined with other data. (Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration, ver. 6.0.2, (April 2014) p. 9)

“Protected Health Information” (PHI) means individually identifiable health information. (45 CFR 160.103).

“Security Incident” means any event (intentional or unintentional) that causes the loss, damage to, destruction, misuse or unauthorized disclosure of CDSS/DHCS information assets.

“Use” means the sharing, employment, application, utilization, examination or analysis of data. (45 CFR 160.103).

IV. CONFIDENTIAL DATA REQUESTS

A. Identification of Confidential Data

The parties agree to identify and share with each other data which is collected and retained by each party pertaining to children or non-minor dependents receiving or previously receiving child welfare services. The only data exchanged will be for the stated purposes in section II, in order to comply with HIPAA. Data will include, but not be limited to, the following categories of information:

- Eligibility Data,
- Demographic Data,
- Social Services Data,
- Medical Data,
- Mental Health Data, and
- Payment Data.

B. Tracking Process for Exchange of Data

Within 30 days of the execution of this MOU, CDSS and DHCS shall develop, following consultation with counties and tribes, and agree upon a written request and response process for the exchange of data between the parties. This process shall include a tracking system for logging each data request, extract, exchange, and match, as applicable. Development and agreement regarding this process shall not forestall data sharing consistent with the terms of this MOU in advance of that process; however, formal record of such data sharing shall be made pursuant to the process once the process has been agreed upon.

At the time of a request for data, the applicable parties shall mutually assess and agree upon the purpose of the data and the intended retention period for the data based upon its purpose and use by the parties. At the expiration of the agreed upon purpose for the data and matched data sets the data shall be returned or destroyed pursuant to the HIPAA Business Associate Addendum (Exhibit A) and the CDSS Confidentiality and Security Requirements (Exhibit C) unless the parties mutually agree in writing to a new purpose and retention period for the data and matched data sets. At minimum, the tracking system shall include:

1. Identification of the individual(s) responsible in each party to receive data and data requests, authorize the exchange or provision of data for his/her party, and be responsible for providing the requested data to the other party.
2. A log that tracks each data set requested, extracted, exchanged and/or matched, under this MOU. The log must include, at a minimum, the following about the data to be exchanged:
 - a) Data elements;
 - b) Population;
 - c) Relevant time period;
 - d) Purpose;
 - e) Request date;
 - f) Delivery date;
 - g) Retention period;
 - h) Frequency of data provision;
 - i) Authority; and
 - j) Person who reviewed and authorized the release, pursuant to the written request.

C. Process for Requesting Data and Matched Data

1. The requesting party shall provide to the providing party's Project Representative identified pursuant to Section B(1) of this MOU a written request for data and/or matched data using prescribed formats and following the agreed upon data request process. The written request shall describe the information requested, including but not limited to the purpose and intended use of the requested data; the authority for the intended use of the data; how the intended use is in accordance with the purposes of this MOU; and who the intended users are.

2. The request shall also include information regarding the following:

- a) Population;
- b) Relevant time period;
- c) Request date;
- d) Delivery date;
- e) Retention period; and
- f) Frequency of data provision;

Upon receipt of the written request, the applicable parties will evaluate the request for completeness, for compliance with this MOU and applicable laws. Requests shall be prioritized, if necessary, at the sole discretion of the data owner, although reasonable effort shall be made to accommodate the needs of the requesting party. If the data or matched data will be provided by the DHCS or CDSS to a county or tribe, then CDSS will coordinate the planning, format, and delivery with the requesting party.

D. Data Sharing between the Parties in Compliance With All Applicable Laws

- 1. Each party shall be responsible for ensuring that any data that is shared, matched, exchanged or used is done so in compliance with all applicable state and federal laws.
- 2. When CDSS is accessing or using confidential data provided by DHCS, CDSS agrees to comply with the provisions of the DHCS HIPAA Business Associate Addendum (Exhibit A), the IEA SSA and DHCS Agreement (Exhibit B.1), attached to this MOU and all Federal and State privacy and security laws.
- 3. When DHCS is accessing and using confidential data provided by CDSS, DHCS agrees to comply with the provisions of the CDSS Confidentiality and Security Requirements for California State Agencies (Exhibit C), the IEA SSA and CDSS Agreement (Exhibit B.2), and all Federal and State privacy and security laws.
- 4. Matched confidential data furnished by CDSS and/or DHCS that is transmitted to other parties to this MOU is subject to the DHCS HIPAA Business Associate Addendum (Exhibit A), CDSS Confidentiality and Security Requirements (Exhibit C), the SSA agreements, (Exhibits B.1 and B.2), and all federal and state privacy and security laws.
- 5. Matched confidential data furnished by any party pursuant to this MOU will be used or disclosed only as specifically provided by this MOU. Matched confidential data furnished by any party pursuant to this MOU shall not be disclosed for use to any person other than the authorized parties' staff who is assigned to the use the data for the purposes authorized under this MOU.
- 6. Each party shall maintain a written record of staff authorized to access and who have accessed (users) the confidential data that has been exchanged pursuant to this MOU. Each party shall provide a copy of its users that have accessed the confidential data provided pursuant to this MOU, to other parties upon request.
- 7. Pursuant to this MOU and for purposes of their respective program responsibilities, either party may transmit confidential data, matched data sets, and reports regarding children or non-minor dependents receiving child welfare services. Data and matched datasets containing confidential data may be shared only for purposes directly connected with the administration of child welfare services or health care services.

When transmitting confidential data to another party, both the sending and receiving party shall comply with all appropriate privacy and security requirements and procedures, including the use of encryption.

E. Data Sharing Activities

The parties shall mutually engage in the following activities to support the data sharing between the parties authorized by this MOU by:

1. Participating in the planning and design of the exchange of data.
2. Providing access to completed data extracts and matches, in a manner and at a time mutually agreed upon.
3. Requesting additional information from the data extracts and matched data sets, as needed by either party for administrative purposes, including verifying and tracking the provision of information or services to applicants for and recipients of programs.

F. Breach Response Process by the Parties for Matched Data

1. The party in possession of the data when the breach occurs and who experiences the breach will be responsible for reporting to all pertinent parties, for complying with all applicable laws, and for all costs and liabilities related to the breach.
2. If CDSS is responsible for a breach, CDSS will report the breach to and comply with DHCS HIPAA Business Associate Addendum (Exhibit A) and the DHCS' SSA agreement (Exhibit B.1).
3. If DHCS is responsible for the breach of CDSS provided data, DHCS will report the breach to and comply with CDSS' Confidentiality and Security Requirements (Exhibit C) and the CDSS SSA agreement (Exhibit B.2).
4. If a county or tribe is responsible for the breach, the county or tribe will be responsible for the breach notifications and reporting the breach to CDSS and DHCS as set forth in the DHCS HIPAA Business Associate Addendum, (Exhibit A); the CDSS Confidentiality and Security Requirements (Exhibit C), and the SSA agreements, (Exhibits B.1 and B.2).
5. The persons to be notified and the process for notice in the event of a breach are identified in the DHCS HIPAA Business Associate Addendum (Exhibit A) and CDSS Confidentiality and Security Requirements (Exhibit C) except that the contact information for CDSS and DHCS are:

Nola Niegel
Acting Information Security Officer
Information Systems Division
California Department of Social Services
744 P Street, M.S. 9-9-70
Sacramento, CA 95814
(916) 654-0694
iso@dss.ca.gov

DHCS Privacy Officer	DHCS Information Security Officer
Privacy Officer c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Fax: (916) 440-5537 Telephone: ITSD Service Desk (916) 440- 7000 or (800) 579- 0874

V. RESPONSIBILITIES FOR DATA DISSEMINATION OUTSIDE OF THE PARTIES OF THE MOU

A. De-identified Data Released to Entities Outside of the Parties

De-identified data or reports containing only de-identified data provided pursuant this MOU to the parties may be transmitted to outside parties. Data shall be de-identified in compliance with HIPAA and other applicable laws and regulations, and the process for de-identification of data provided herein.

B. Data Sharing by Parties with Authorized Entities or Contractors

Parties to this MOU may provide confidential or de-identified data, including matched data, to authorized entities or contractors that have contracted with the parties for the provision of program services to children or non-minor dependents receiving child welfare services if the parties have determined that it is necessary for their ongoing, administration, oversight, monitoring, evaluation, and reporting responsibilities. All such contracts must include the Exhibits to this MOU. All data provided to authorized entities or contractors shall meet the minimum necessary requirements of HIPAA.

C. Articles for Publication

1. CDSS/DHCS

CDSS and DHCS may participate in the writing and reviewing of each other's reports and articles that refer to or include information regarding the subject matters of this MOU that are intended for publication. For the purpose of this MOU, publication means that an article or report is intended to be provided or made available to the general public. This includes posting reports, articles or data on the Internet or in any other public medium or forum. Only de-identified information as defined by HIPAA shall be used for publishing reports and/or articles that may or are made available to the public. The process for de-identified data provided herein shall be used by the departments for reaching mutual agreement on articles and reports for publication. This paragraph does not apply, and mutual agreement by CDSS and DHCS is not required, for reports (such

as outcome measures) that are produced by CDSS or DHCS in the ordinary course of the operation or administration of their own programs using only data in their respective systems.

2. County or Tribe

Matched confidential data released to counties shall not be used for publications produced by the counties or tribes. Only de-identified information as defined by HIPAA shall be used for publishing reports and/or articles that may or are made available to the public.

D. Other Special Reports and Analyses by the Parties

The parties may develop other special reports such as regional/geographic analyses, demographic variations, and so forth under this MOU for each party's internal use. Only de-identified data shall be included in any published analyses or reports.

E. Process for De-identification

1. CDSS/DHCS

Each Department is responsible for determining the sufficiency of the HIPAA de-identification determination for its intended use of the de-identified data by the Department. Prior to implementing the intended use of the de-identified data each Department agrees to provide to the other Department for review, the proposed de-identified data to be used. If the reviewing Department disagrees with the de-identification determination that has occurred, the reviewing Department shall notify the Department of its assessment and objections within five working days of receiving the de-identified data. If the Departments cannot agree within 10 working days following the notification of objections to the de-identified data, the matter shall immediately be referred to the first level of the Dispute Resolution Process using the Form, Exhibit D.

2. County or Tribe

Each county or tribe is responsible for determining the sufficiency of the HIPAA de-identification determination for its intended use of the de-identified data by the county or tribe. Prior to the intended use of the de-identified data the county or tribe agrees to provide to the Departments relevant information related to the de-identification. If either of the Departments disagrees with the de-identification determination of the county or tribe that has occurred and the parties cannot agree within 10 working days, the matter shall immediately be referred to the first level of the County or Tribe Dispute Resolution Process using the Form, Exhibit D.

F. Miscellaneous Requests for Data – PRA

1. CDSS/DHCS

In the event either Department receives a Public Records Act (PRA) request, a subpoena, litigation-related request, or any other request for the confidential information that is the subject of this MOU and not otherwise provided for herein, the Department receiving the request shall immediately notify the other Department and meet and confer as necessary on the appropriate response to the request.

2. County or Tribe

In the event that a County or Tribe receives a Public Records Act (PRA) request, a subpoena, litigation-related request, or any other request for the confidential information that is the subject of this MOU and not otherwise provided for herein, the county or tribe shall immediately notify the Project Representatives of both Departments and meet and confer as necessary on the appropriate response to the request.

G. Consent - CDSS/DHCS

If any issues of whether consent is needed from children or non-minor dependents receiving child welfare services before confidential data can be used or shared with third parties for the purposes of this MOU, DHCS and CDSS agree to meet and confer, and within 30 days to mutually agree, on a form or process for gaining the consent of the children or non-minor dependents receiving child welfare services or the child's representative.

H. Existing Data Use Agreements Between CDSS and DHCS

At the time of the execution of this MOU, there are existing data use agreements between CDSS and DHCS directly related to the purposes of this MOU. These existing agreements shall continue in full force and effect until their expiration, at which time their purposes and provisions shall be incorporated into and made a part of this MOU as though fully set forth herein.

VI. TERM

A. CDSS/DHCS

The term of this MOU shall commence upon the approval and signature of the Director of both Departments and shall continue in effect until cancelled by either Department. Written notice of cancellation shall be provided by the cancelling Department to the other Department no later than 180 days prior to the specified cancellation date.

B. County or Tribe

The term of this MOU with each county or tribe shall commence upon the approval and signature of the County or Tribe and continue in effect until cancelled by the Departments or County or Tribe. Written notice of cancellation shall be provided by the cancelling party to the Department(s), county or tribe or by the Department(s) to the county or tribe no later than 180 days prior to the specified cancellation date.

VII. PAYMENT

There is no compensation payable to any of the parties in connection with this MOU.

VIII. AMENDMENT PROCESS

A. Non-Substantive Changes by the Parties

Any party may propose written non-substantive changes or revisions to the information, activities and tasks of this MOU without amendment provided such changes do not alter the

overall goals and basic purpose of the MOU. The changes will be effective upon the mutual agreement of the affected parties. The addition of individual Counties or Tribes to this MOU, as provided herein, shall be a non-substantive change and shall not require a formal amendment.

B. Substantive Changes by the Parties

A party, during the term of this MOU, may propose a substantive change or amendment to the terms of this MOU. Such changes or amendments shall be proposed in writing to the other parties, and the parties agree to meet and confer within 10 working days to discuss or negotiate the proposed changes. The agreed-upon changes to this MOU shall be made through an expedited amendment process that will be reviewed and approved by each party's executive, program and legal staff and signed by the party's Director or designee. The expedited amendment will be completed and processed within 30 days unless this time is extended by the parties. This expedited amendment shall be binding on all parties upon the approval and signature of the parties' Directors or their designee.

IX. DISPUTE RESOLUTION PROCESS

A. CDSS/DHCS

If a dispute arises between DHCS and CDSS, the Departments must seek resolution using the process outlined below.

1. The aggrieved department should first informally discuss the problem with the Project Representative and Contract Manager of the other Department. If the problem cannot be resolved informally, the aggrieved Department must direct the grievance together with any evidence, in writing, to the Chief Deputy Director of the other department. The grievance must state the issues in dispute, the legal authority or other basis for the Department's position and the remedy sought. The Chief Deputy Director must render a decision within ten (10) working days after receipt of the written grievance. The Chief Deputy Director shall respond in writing to the aggrieved Department indicating his/her decision and the reason(s) therefore. Should the aggrieved Department disagree with the Chief Deputy Director's decision, the aggrieved Department may appeal to the second level.
2. When appealing to the second level the aggrieved Department must prepare an appeal indicating the reasons for disagreement with the Chief Deputy Director's decision. The aggrieved Department shall include with its appeal a copy of its original statement of dispute along with any supporting evidence and a copy of the Chief Deputy Director's decision. The appeal shall be addressed to the Health and Human Services Agency (HHSA) Secretary or his/her designee within ten (10) working days from receipt of the Chief Deputy Director's decision. The HHSA Secretary or his/her designee shall meet with the aggrieved Department to review the issues raised. A written decision signed by the HHSA Agency Secretary or his/her designee shall be directed to the aggrieved Department within twenty (20) working days of receipt of the second level appeal.

B. County or Tribe

If a dispute arises between the Departments and a County or Tribe, the County or Tribe must seek resolution using the process outlined below.

1. The aggrieved party should first informally discuss the problem with the Project Representative and Contract Manager of the other party. If the problem cannot be resolved informally, the aggrieved party must direct the grievance together with any evidence, in writing, to the Program Branch Chief of the Project Representative for Department(s) or designee for the Tribe or County, as applicable. The grievance must state the issues in dispute, the legal authority or other basis for the party's position and the remedy sought. The party receiving the grievance must render a decision within ten (10) working days after receipt of the written grievance of the other party. The grievance shall be responded to in writing to the aggrieved party indicating their decision and reasons therefore. Should the aggrieved party disagree with the decision, the aggrieved party may appeal to the second level.
2. When appealing to the second level the aggrieved party must prepare an appeal indicating the reasons for disagreement with the decision by the other party. The aggrieved party shall include with its appeal a copy of their original statement of dispute along with any supporting evidence and a copy of the prior decision of the other party. The aggrieved party shall address the appeal to the other party's second level appeal designee within ten (10) working days from receipt of the written decision of the other party. (For the Departments the second level appeal designee will be the Deputy Director of the division in which the branch is organized, or his/her designee; for the County or Tribe the second level appeal will be to the County or Tribes designee.) The second level appeal designee shall meet with the aggrieved party to review the issues raised. A written decision signed by the second level appeal designee shall be directed to the aggrieved party within twenty (20) working days of receipt of the second level appeal.

X. SURVIVAL

The privacy, confidentiality, and security provisions of this MOU survive the termination or expiration of this MOU.

XI. INCORPORATED EXHIBITS

The following exhibits are incorporated herein, and made a part hereof by this reference:

1) Exhibit A	HIPAA Business Associate Addendum	15 pages
2) Exhibit B.1	IEA SSA and DHCS Agreement	74 pages
3) Exhibit B.2	IEA SSA and CDSS Agreement	77 pages
4) Exhibit C	CDSS Confidentiality and Security Requirements for California State Agencies	6 pages
5) Exhibit D	Form for Dispute Resolution	1 page

XII. PROJECT REPRESENTATIVES AND SIGNATORIES

The project representatives during the term of this MOU from the California Department of Social Services will be:

Project Representative	Contract Manager
Akhtar Khan Branch Chief or designee Research Services Branch (916) 653-1800 Akhtar.Khan@dss.ca.gov	Alicia Sandoval Child Welfare and Data Analysis Bureau Research Services Branch (916) 653-1812 Alicia.Sandoval@dss.ca.gov

The project representatives during the term of this MOU from the California Department of Health Care Services will be:

Project Representative	Contract Manager
Linette Scott Deputy Director or designee Information Management Division (916) 440-7639 Linette.Scott@dhcs.ca.gov	Angelique Lastinger Information Management Division (916) 332-8573 Angelique.Lastinger@dhcs.ca.gov

Either department may make changes to the project representatives above by giving written notice to the other party. Said changes shall not require an amendment to this Agreement. Each County or Tribe signing this MOU will designate and identify to the Departments the Project Representative for the County or Tribe that will be the single point of contact with the Departments for County or Tribe to receive and make requests for data to the Departments.

XIII. COUNTY AND TRIBE - PROJECT REPRESENTATIVES AND SIGNATORIES

By signing this MOU, the County or Tribe signatory represents that he or she has authority to bind and obligate the specific County or Tribe the signatory represents. On behalf of the County or Tribe the signatory agrees to the terms, conditions and obligations of this MOU including but not limited to ensuring the integrity, security, and confidentiality of all data provided by the Departments. In addition, the signatory is responsible for permitting disclosure or any distributions of the data to other County or Tribe entities or users and to permit only those disclosures and uses that are consistent with this MOU and as permitted by law.

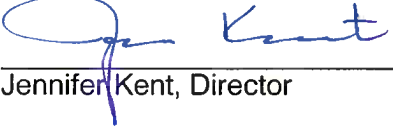
This Memorandum of Understanding is not effective until signed by all parties.

California Department of Social Services

By: 
Will Lightbourne, Director

Date: 4/8/15

California Department of Health Care Services

By: 
Jennifer Kent, Director

Date: 4/8/15

SIGNATURE PAGE FOR COUNTY

This Memorandum of Understanding is not effective until signed by all parties.

By: _____

Date: _____

SIGNATURE PAGE FOR TRIBE

This Memorandum of Understanding is not effective until signed by all parties.

By: _____

Date: _____

Exhibit A**HIPAA Business Associate Addendum****I. Recitals**

- A. This Contract (Agreement) has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").
- B. The Department of Health Care Services ("DHCS") wishes to disclose to Business Associate certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.
- C. As set forth in this Agreement, Contractor, here and after, is the Business Associate of DHCS acting on DHCS' behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of DHCS and creates, receives, maintains, transmits, uses or discloses PHI and PI. DHCS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties."
- D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that DHCS must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act, and the Final Omnibus Rule as well as the Alcohol and Drug Abuse patient records confidentiality law 42 CFR Part 2, and any other applicable state or federal law or regulation. 42 CFR section 2.1(b)(2)(B) allows for the disclosure of such records to qualified personnel for the purpose of conducting management or financial audits, or program evaluation. 42 CFR Section 2.53(d) provides that patient identifying information disclosed under this section may be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by an appropriate court order.
- E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

II. Definitions

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the Final Omnibus Rule.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the final Omnibus Rule.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and Final Omnibus Rule.
- D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.

Exhibit A**HIPAA Business Associate Addendum**

- E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.
- F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.
- G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164.
- H. Personal Information shall have the meaning given to such term in California Civil Code section 1798.29.
- I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.
- J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.
- M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act, and the HIPAA regulations.

III. Terms of Agreement**A. Permitted Uses and Disclosures of PHI by Business Associate**

Permitted Uses and Disclosures. Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of DHCS, provided that such use or disclosure would not violate the

Exhibit A**HIPAA Business Associate Addendum**

HIPAA regulations, if done by DHCS. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, the HIPAA regulations, the Final Omnibus Rule and 42 CFR Part 2.

1. ***Specific Use and Disclosure Provisions.*** Except as otherwise indicated in this Addendum, Business Associate may:
 - a. ***Use and disclose for management and administration.*** Use and disclose PHI for the proper management and administration of the Business Associate provided that such disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.
 - b. ***Provision of Data Aggregation Services.*** Use PHI to provide data aggregation services to DHCS. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of DHCS with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of DHCS.

B. Prohibited Uses and Disclosures

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).
2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of DHCS and as permitted by 42 U.S.C. section 17935(d)(2).

C. Responsibilities of Business Associate

Business Associate agrees:

1. ***Nondisclosure.*** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by this Agreement or as required by law.
2. ***Safeguards.*** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of DHCS, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities, and

Exhibit A**HIPAA Business Associate Addendum**

which incorporates the requirements of section 3, Security, below. Business Associate will provide DHCS with its current and updated policies.

3. **Security.** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
 - a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;
 - b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement;
 - c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and
 - d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of this Agreement.

Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with DHCS.

- D. Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

E. Business Associate's Agents and Subcontractors.

1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of DHCS, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act the HIPAA regulations, and the Final Omnibus Rule, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI and PI. Business associates are directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. Business Associate shall incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PI be reported to Business Associate.

Exhibit A**HIPAA Business Associate Addendum**

2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:
 - a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by DHCS; or
 - b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

F. Availability of Information to DHCS and Individuals. To provide access and information:

1. To provide access as DHCS may require, and in the time and manner designated by DHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to DHCS (or, as directed by DHCS), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for DHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DHCS health plans; or those records used to make decisions about individuals on behalf of DHCS. Business Associate shall use the forms and processes developed by DHCS for this purpose and shall respond to requests for access to records transmitted by DHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.
2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable DHCS to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).
3. If Business Associate receives data from DHCS that was provided to DHCS by the Social Security Administration, upon request by DHCS, Business Associate shall provide DHCS with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

G. Amendment of PHI. To make any amendment(s) to PHI that DHCS directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner designated by DHCS.**H. Internal Practices.** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from DHCS, or created or received by Business Associate on behalf of DHCS, available to DHCS or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by DHCS or by the Secretary, for purposes of determining DHCS' compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to DHCS and shall set forth the efforts it made to obtain the information.

Exhibit A**HIPAA Business Associate Addendum**

I. Documentation of Disclosures. To document and make available to DHCS or (at the direction of DHCS) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for DHCS as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for DHCS after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

J. Breaches and Security Incidents. During the term of this Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

1. **Notice to DHCS.** (1) To notify DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to DHCS by the Social Security Administration. This notification will be **by telephone call plus email or fax** upon the discovery of the breach. (2) To notify DHCS **within 24 hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to DHCS by the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link:

<http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx>

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

- a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
- b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

Exhibit A**HIPAA Business Associate Addendum**

2. ***Investigation and Investigation Report.*** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. If the initial report did not include all of the requested information marked with an asterisk, then within 72 hours of the discovery, Business Associate shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer:
3. ***Complete Report.*** To provide a complete report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. If all of the required information was not included in either the initial report, or the Investigation Report, then a separate Complete Report must be submitted. The report shall be submitted on the "DHCS Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide DHCS with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "DHCS Privacy Incident Report" form. DHCS will review and approve or disapprove the determination of whether a breach occurred, is reportable to the appropriate entities, if individual notifications are required, and the corrective action plan.
4. ***Notification of Individuals.*** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.
5. ***Responsibility for Reporting of Breaches.*** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach immediately upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DHCS in addition to Business Associate, Business Associate shall notify DHCS, and DHCS and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.
6. ***DHCS Contact Information.*** To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated herein. DHCS reserves the right to make changes to

Exhibit A
HIPAA Business Associate Addendum

the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

DHCS Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646 Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Fax: (916) 440-5537 Telephone: EITS Service Desk (916) 440-7000 or (800) 579-0874

K. Termination of Agreement. In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by DHCS of this Addendum, it shall take the following steps:

1. Provide an opportunity for DHCS to cure the breach or end the violation and terminate the Agreement if DHCS does not cure the breach or end the violation within the time specified by Business Associate; or
2. Immediately terminate the Agreement if DHCS has breached a material term of the Addendum and cure is not possible.

L. Due Diligence. Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.

M. Sanctions and/or Penalties. Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

IV. Obligations of DHCS

DHCS agrees to:

A. Notice of Privacy Practices. Provide Business Associate with the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR section 164.520, as well as any changes to such notice. Visit the DHCS Privacy Office to view the most current Notice of Privacy Practices at: <http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/default.aspx> or the DHCS website at www.dhcs.ca.gov (select "Privacy in the left column and "Notice of Privacy Practices" on the right side of the page).

B. Permission by Individuals for Use and Disclosure of PHI. Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.

Exhibit A**HIPAA Business Associate Addendum**

- C. *Notification of Restrictions.*** Notify the Business Associate of any restriction to the use or disclosure of PHI that DHCS has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- D. *Requests Conflicting with HIPAA Rules.*** Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations if done by DHCS.

V. Audits, Inspection and Enforcement

- A.** From time to time, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the DHCS Privacy Officer in writing. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does DHCS':
1. Failure to detect or
 2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of DHCS' enforcement rights under this Agreement and this Addendum.
- B.** If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify DHCS and provide DHCS with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

VI. Termination

- A. *Term.*** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the contract and shall terminate when all the PHI provided by DHCS to Business Associate, or created or received by Business Associate on behalf of DHCS, is destroyed or returned to DHCS, in accordance with 45 CFR 164.504(e)(2)(ii)(I).
- B. *Termination for Cause.*** In accordance with 45 CFR section 164.504(e)(1)(ii), upon DHCS' knowledge of a material breach or violation of this Addendum by Business Associate, DHCS shall:
1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by DHCS; or
 2. Immediately terminate this Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.

Exhibit A**HIPAA Business Associate Addendum**

- C. *Judicial or Administrative Proceedings.*** Business Associate will notify DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. DHCS may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. DHCS may terminate this Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.
- D. *Effect of Termination.*** Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from DHCS (or created or received by Business Associate on behalf of DHCS) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify DHCS of the conditions that make the return or destruction infeasible, and DHCS and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

VII. Miscellaneous Provisions

- A. *Disclaimer.*** DHCS makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.
- B. *Amendment.*** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon DHCS' request, Business Associate agrees to promptly enter into negotiations with DHCS concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. DHCS may terminate this Agreement upon thirty (30) days written notice in the event:
1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by DHCS pursuant to this Section; or
 2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that DHCS in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.
- C. *Assistance in Litigation or Administrative Proceedings.*** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.

Exhibit A

HIPAA Business Associate Addendum

- D. *No Third-Party Beneficiaries.*** Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than DHCS or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
- E. *Interpretation.*** The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.
- F. *Regulatory References.*** A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.
- G. *Survival.*** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of this Agreement.
- H. *No Waiver of Obligations.*** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

Exhibit A**HIPAA Business Associate Addendum****Attachment A****Business Associate Data Security Requirements****I. Personnel Controls**

- A. *Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of DHCS, or access or disclose DHCS PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
- B. *Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. *Confidentiality Statement.*** All persons that will be working with DHCS PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.
- D. *Background Check.*** Before a member of the workforce may access DHCS PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

II. Technical Security Controls

- A. *Workstation/Laptop encryption.*** All workstations and laptops that process and/or store DHCS PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.
- B. *Server Security.*** Servers containing unencrypted DHCS PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. *Minimum Necessary.*** Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. *Removable media devices.*** All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

Exhibit A**HIPAA Business Associate Addendum**

- E. *Antivirus software.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- F. *Patch Management.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
- G. *User IDs and Password Controls.*** All users must be issued a unique user name for accessing DHCS PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
- Upper case letters (A-Z)
 - Lower case letters (a-z)
 - Arabic numerals (0-9)
 - Non-alphanumeric characters (punctuation symbols)
- H. *Data Destruction.*** When no longer needed, all DHCS PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.
- I. *System Timeout.*** The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- J. *Warning Banners.*** All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. *System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- L. *Access Controls.*** The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

Exhibit A**HIPAA Business Associate Addendum**

- M. *Transmission encryption.*** All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.
- N. *Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

III. Audit Controls

- A. *System Security Review.*** All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.
- B. *Log Reviews.*** All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
- C. *Change Control.*** All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

IV. Business Continuity / Disaster Recovery Controls

- A. *Emergency Mode Operation Plan.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.
- B. *Data Backup Plan.*** Contractor must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

V. Paper Document Controls

- A. *Supervision of Data.*** DHCS PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. *Escorting Visitors.*** Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

Exhibit A

HIPAA Business Associate Addendum

- C. Confidential Destruction.** DHCS PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. Removal of Data.** DHCS PHI or PI must not be removed from the premises of the Contractor except with express written permission of DHCS.
- E. Faxing.** Faxes containing DHCS PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.
- F. Mailing.** Mailings of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DHCS to use another method is obtained.

California Department of Social Services (CDSS)
Confidentiality and Security Requirements for
CALIFORNIA STATE AGENCIES
Interagency Agreements/Memoranda of Understanding

I. GENERAL REQUIREMENTS

- A. These requirements provide a framework for maintaining the confidentiality and security of confidential data the State agency gathers or processes in the course of carrying out the terms of this agreement with CDSS. Definitions of commonly used terms are provided. For purposes of this agreement only, confidential and/or personal data are referred to as *confidential data*.
- B. No exceptions from these policies shall be permitted without the explicit, prior, written approval of authorized CDSS staff. All confidentiality and security requirements, as stated in this agreement, shall be enforced and continue throughout the term of the agreement. Data protection and security plans may be required prior to receipt of confidential data.
- C. In addition, the State agency will be expected to demonstrate that it has taken specific steps to ensure the data is kept secure and confidential.

II. PRIVACY, SECURITY, AND CONFIDENTIALITY

- A. All confidential data made available in order to carry out this Agreement, will be protected from unauthorized use and disclosure through the observance of the same or more effective means as that required by the State Administrative Manual Sections 5300-5399, Civil Code Section 1798 et seq., Welfare and Institutions Code Section 10850, and other applicable federal and/or State laws governing individual privacy rights and data security. Upon request, CDSS reserves the right to review, and then accept security and privacy procedures that are relevant to its data.
- B. The State agency is responsible for the security of the confidential data and compliance with the terms of this agreement by its employees, contractors, or sub-contractors.

III. ACCEPTABLE USE AND DISCLOSURE

- A. The State agency shall not use or further disclose confidential data other than as permitted or required by this agreement.
- B. The State agency shall refer any persons not included under this agreement with CDSS, to CDSS to request access to the confidential data.
- C. The State agency agrees that the information obtained will be kept in the strictest confidence and shall make information available to its own employees only on a "need to know" basis. Need to know is based on those authorized employees who need information to perform their official duties in connection with the uses of the information authorized by this agreement.

IV. INFORMATION SECURITY INCIDENTS

- A. Notification: The State agency shall notify the CDSS or its designated agent of any actual or attempted information security incidents, as defined below, within 24 hours of initial detection. Information security incidents shall be reported by telephone to:

Nola Niegel
Acting Information Security Officer
Information Systems Division
California Department of Social Services
744 P Street, M.S. 9-9-70
Sacramento, CA 95814
(916) 654-0694

- B. Cooperation: The State agency shall cooperate in any investigations of information security incidents.
- C. Isolation: The system or device affected by an information security incident, and containing CDSS confidential data, shall be removed from operation immediately to the extent necessary to prevent further harm or unauthorized disclosures. It shall remain removed from operation until correction and mitigation measures have been applied. CDSS must be contacted prior to placing the system or device, containing CDSS confidential data, back in operation. The affected system or device, containing CDSS confidential data, shall not be returned to operation until CDSS gives its approval.

V. ENCRYPTION AND TRANSMISSION

- A. The State agency shall ensure the confidentiality of CDSS data transmission.
- B. The State agency shall ensure that all electronic file media used in data exchanges are either:
1. Transferred by secure file transfer protocol; or
 2. Encrypted or protected with equally strong measures if placed on any personal computer (either desktop or laptop), or on any removable storage media of any kind, pursuant to Budget Letter 05-32.
- C. Transmission of CDSS confidential data by fax shall not be used unless no other method of transmission is feasible and with the following pre-cautions:
1. Faxes containing CDSS confidential data shall not be left unattended.
 2. Fax machines shall be in secure areas.
 3. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them.
 4. Fax numbers shall be verified with the intended recipient before sending

- D. Transfer of CDSS confidential data via paper copy shall be mailed using a secure, bonded mail service, such as Federal Express, Golden State Overnight or by registered U.S. Mail (i.e., accountable mail using restricted delivery). All packages must be double packed with a sealed envelope and a sealed outer envelope or locked box.

VI. NETWORK SECURITY

- A. CDSS confidential data shall be secured against logical or physical access on any computing device, on any storage media, or in transit.
- B. Maintaining a firewall separating any network attached computing device containing the data from any network not controlled by the contractor.
- C. Using password based authentication and other security safeguards and precautions to restrict logical and physical access to the data to authorized users only.
- D. Maintaining a log of all accesses to the data.
- E. Restricting removal of the data from the work location.
- F. Applying all vendor supplied security patches and updates to all computing devices containing or having access to the data.
- G. Configuring all computing devices containing or having access to the data in a secure manner including:
 - 1. Requiring the authentication or re-authentication after an established period of inactivity.
 - 2. Not allowing remote access to CDSS confidential data or the server that stores it unless:
 - a. The remote computer is physically secure and located in manner to ensure the privacy of the data displayed or stored on it.
 - b. Communication to the server must be on a physically secured dedicated line, through a remote control solution using SSL encryption, or through a strongly encrypted VPN with firewalls that do not permit split tunneling, not on a public network.
 - c. The remote computer accessing CDSS data must be owned and controlled by the contractor and must not be configured in a less secure manner than the contractor's internal computers.

VII. RETURN OR DESTRUCTION OF DATA

- A. Return or Destruction: Confidential data used, compiled, processed, stored or derived by the State agency in the performance of this agreement shall be destroyed or returned by the agency. All such data shall either be returned to

CDSS in an agreed-upon format within 30 days of termination of this contract or be destroyed, unless this agreement expressly authorizes the State agency to retain specified confidential data after the termination of this agreement. If the data is returned to CDSS, the State agency shall provide CDSS with the media and an inventory of the data and files returned.

- B. For purposes of this subsection, "derived" confidential data shall refer to a data set, containing confidential data, that is derived from another data set by (a) elimination of fields from the original data set, (b) addition of fields to the original data set, (c) manipulation of the structure of the original data set or a derivative data set, or (d) renaming an original data set.
- C. **Methods of Destruction:** The State agency shall destroy all confidential data not returned when the use authorized ends in accordance with approved methods of confidential destruction (via shredding, burning, certified or witnessed destruction, or degaussing of magnetic media). All computer sets containing individual identifiers shall be destroyed. The agency shall use wipe software on all the hard drive surfaces of computers used to process or store CDSS confidential data when the computer is withdrawn from use in processing or storing such data. This includes back-up media. Destruction shall occur before the effective date of termination of this contract and a letter of confirmation shall be provided to CDSS detailing when, how, and what CDSS data was destroyed. This certification letter is required whether destruction services are contracted or the agency performs the destruction.

VIII. CONFIDENTIALITY AND SECURITY COMPLIANCE STATEMENT

Based on the requirements of the Welfare and Institutions Code Section 10850, Civil Code Section 1798 et seq., and State Administrative Manual Sections 5300-5399, the State agency shall provide security sufficient to ensure protection of confidential information from improper use and disclosures, including sufficient administrative, physical, and technical safeguards to protect personal information from reasonable anticipated threats to the security or confidentiality of the information.

AGREEMENT NUMBER: _____

NAME OF STATE AGENCY: _____

<i>*Signature of Authorized State Official</i>	
<i>Title:</i>	<i>Date:</i>
<i>Phone:</i> <i>Fax:</i>	<i>E-Mail Address:</i>
<i>*Title: Information Security Officer Signature</i>	<i>Date:</i>
<i>Phone:</i> <i>Fax:</i>	<i>E-Mail Address:</i>

** Signatures are required by the Information Security Officer and Authorized State Official. This may include the Agency Chief Information Officer, System Administrator, or other individual responsible for ensuring compliance with the confidentiality and security requirements.*

IX. DEFINITIONS

For the purposes of these requirements, the stated terms are defined as noted:

State Agency: For purposes of this agreement, the terms State agency, agency, or contractor, refers to the California State agency with which CDSS enters into this agreement.

Confidential Data: Information, the disclosure of which is restricted or prohibited by any provision of law. Some examples of “confidential information” include, but are not limited to, public social services client information described in California Welfare and Institutions Code Section 10850 and “personal information” about individuals as defined in California Civil Code Section 1798.3 of the Information Practices Act (IPA) if the disclosure of the “personal information” is not otherwise allowed by the IPA. Confidential data includes personal identifiers. For purposes of this agreement only, confidential and/or personal data are referred to as *confidential data*

Confidential Identifiers: Are specific personal identifiers such as name, social security number, address and date of birth.

De-Identification: Removal of personal identifiers. Examples of personal identifiers include name, social security numbers, driver’s license numbers, and account numbers with access codes. Personal information does not include publicly available information that is lawfully made available to the general public. (See definitions for confidential data and confidential/ personal identifiers.)

Information Assets: Information assets include anything used to process or store information, including (but not limited to) records, files, networks, and databases; information technology facilities, equipment (including personal computer systems), and software (owned or leased).

Information Security Incidents: Information Security incidents include, but are not limited to, the following; any event (intentional or unintentional) that causes the loss, damage to, destruction, or unauthorized disclosure of CDSS information assets.

Risk: The likelihood or probability that a loss of information assets or breach of security will occur.

Signature of Authorized State Official: Authorized signature shall be determined by the state agency. It is recommended that the agency ISO or individual responsible for oversight of the security requirements in the agreement, review and sign the compliance statement.

EXHIBIT D

Dispute Resolution regarding the Health Insurance Portability and Accountability Act (HIPAA) De-identification of Data 45 CFR 164.514(a) and b(1) and b(2)

1. Describe the study or intended use of the data, (authority for data use, purpose, and subject population described in the data elements) that has been de-identified pursuant to HIPAA regulations

2. Describe the de-identification method or procedures engaged in to make the determination the data is properly de-identified

3. Describe the objections to the de-identification method(s) used or an explanation why there is a reasonable basis to believe that the data can be used to identify an individual

4. Response that de-identification meets HIPAA requirements and/or there is no reasonable basis to believe data can be used to identify an individual.

Attach any documents that are relevant to resolving the dispute.

New York City Inter-Agency Data Exchange Agreement

Inter-Agency Data Exchange Agreement

This Inter-Agency Data Exchange Agreement (hereafter referred to as "Agreement") is in furtherance of Executive Order No. 114 of 2008 (Attachment A), issued by the Mayor of the City of New York which established HHS-Connect to facilitate data integration and exchange between existing agency-based information management systems in accordance with all applicable federal, state and local laws, and regulations.

Whereas, in support of Executive Order No. 114, the Agreement sets forth a common set of terms and conditions in support of secure interoperable data exchange between and among health and human services agencies and related agencies.

Whereas, the undersigned agencies have agreed to receive and/or provide data from the data source systems below and have, jointly with HHS-Connect, established applications and infrastructure with which to share data to improve services to the citizens of New York City.

Whereas, the undersigned agencies recognize that many New Yorkers qualify for and participate in multiple City programs. Leveraging advances in modern technology will break down information silos and:

- Improve client outcomes
- Increase reliability of data
- Reduce duplication of client data
- Improve integration of client services
- Promote a client-centric approach to service delivery
- Improve accessibility and management of information
- Improve program effectiveness, performance, and accountability

The Data Source systems currently available through HHS-Connect are as follows:

- 1) New York City Administration for Children's Services (ACS) - Automated Child Care Information Systems (ACCIS)
- 2) New York City Department of Finance (DOF) – Senior Citizen Rent Increase Exemption System (SCRIE)
- 3) New York City Department of Homeless Services (DHS) - Client Tracking System (CTS)
- 4) New York City Housing Authority (NYCHA) - Tenant Data System (TDS)
- 5) New York City Human Resources Administration (HRA)
 - Enterprise Data Warehouse (HRA EDW) – Food Stamp, Public Assistance, Medicaid
 - HRA Document Management Repository

I. DEFINITIONS/DEFINED TERMS

Authentication Authentication is the process by which a user accessing a system demonstrates that he or she is in fact an entity that is associated with an identity previously registered in the system. Authentication does not apply solely to users; it can also be applied at the system or service level (e.g., by user group, agency) and can be used to identify one system or service to another.

Authorized User The term Authorized User is used to identify individuals approved and designated to access Worker Connect. Authorized Users receive rights to access Worker Connect from their individual Participant Agency which is solely responsible for the provisioning and de-provisioning of its employees. In granting access, such Participant Agency affirms such individuals are authorized to access information based upon their functions and responsibilities consistent with their participation in HHS-Connect and approved business use cases.

Business Use Case A business use case includes a description of the functions and responsibilities of an agency, division and/or unit, the information requested and the purpose and intended use of the information. A business use case may include, but is not limited to: (i) a brief description of each user group's business function within its agency, including key roles and responsibilities of staff; (ii) individual scenarios describing how staff would make use of the data within their current business processes (i.e., how workers currently access this data, if applicable, and the manner in which the data is currently used); (iii) the purpose for which the data would be used; and (iv) a description of the added value and benefit of accessing the requested data. Each use case also includes an associated list of relevant data sources, data categories, and/or documents supporting use case scenarios.

Common Client Index (CCI) CCI contains demographic information about a client and has links to all of the data source systems that contain information or documentation about that client. The CCI enables the matching of client records across different Participant data source systems. The CCI facilitates the automation of the client match process based on predefined rules and establishes logical links for the matched records.

Data As used in this Agreement, data shall mean any and all information that is transmitted via HHS-Connect, including documents.

Data Protection Multiple technologies have been deployed with data protection capabilities including, but not limited to: 1) specific access controls; 2) field by field redaction; 3) upstream and downstream filtering; 4) encryption; and 5) filtering logic to restrict quantity of data provided.

Data Provider Data provider means a Participant that provides information from specified data source systems to HHS-Connect applications and infrastructure for use through the CCI, the Document Management Federation, and/or Worker Connect. These can be data source systems both within and outside the HHS domain (including, but not limited to systems/applications of other entities such as federal, state and local or other entity systems/applications).

Data Recipient shall mean a Participant Agency and its specific Authorized User groups,

each of which have been approved to access information from a Participant Data Provider's data source system.

Data Source Systems shall mean individual data source system(s) from Participant Data Providers. This Agreement acknowledges and anticipates that additional data source systems will be added in support of the continued development of HHS-Connect. These may be agency systems within and outside the HHS domain or other state or other governmental or other entity systems/applications that will provide data to the CCL.

Document Management Document Management provides the capability to retrieve client provided documents from participating agency repositories. The Document Management system integrates technology, access controls, and taxonomy to provide an integrated view of documents provided through HHS-Connect.

DoITT The Department of Information Technology & Telecommunications.

Executive Steering Committee (ESC) The ESC, established by the Office of the Deputy Mayor for Health and Human Services, serves as the governance body for facilitating collaboration and providing project guidance.

HHS-Connect A Program established pursuant to Executive Order No. 114 to facilitate data integration and exchange. HHS-Connect is a technology solution that connects clients, agencies, and providers utilizing ground-breaking and innovative technologies to improve the City's ability to serve its population.

HHS-Connect CIO HHS Connect CIO acts in the capacity of CIO for Health and Human Services and as Executive Director of HHS-Connect.

HHS Agencies Referred to collectively as "HHS Agencies" in Executive Order No. 114 as among the agencies providing health and human services: Administration for Children's Services; Department for the Aging; Department of Correction; Department of Health and Mental Hygiene; Department of Homeless Services; Department of Juvenile Justice; Department of Probation; Health and Hospitals Corporation; and Human Resources Administration.

Participant shall mean a Data Provider and/or Data Recipient participating in HHS-Connect. DoITT is a Participant Agency for the sole purpose of maintenance of the systems of HHS-Connect.

Permitted Uses Access and use of data provided as part of HHS-Connect are restricted to Authorized Users of Worker Connect. Data shall be held confidential and shall only be used for authorized purposes directly related to the carrying out of Authorized Users' functions and responsibilities consistent with their agency's participation in HHS-Connect, as documented in Data Recipient's business use case(s).

Provisioning Provisioning refers to Participant Data Recipient agencies providing access

privileges to Worker Connect to Authorized Users.

Role Based Access refers to a method for enforcing access to system functionality and data sets based on the roles individual users play as part of an organization. The method of assigning access, also known as Role Based Access Control (RBAC), uses roles defined to correspond to various job functions.

User Group A unit/division within a Participant Data Recipient Agency authorized to access information from Participant Data Provider data source systems. Access is based upon approval from Data Provider's counsel in accordance with all applicable laws and regulations.

Worker Connect A web-based system that enables Authorized Users to access multiple data sources through one point of entry. The system is a secure system where a single query can gather information from many different data sources and display the information in a user friendly format. Worker Connect consolidates data from CCI, Document Management system, and data source systems.

II. PURPOSE AND SCOPE

The purpose of this Agreement is to set forth the terms and conditions of use of data shared through HHS-Connect applications and infrastructure to ensure the effective and secure exchange of data.

III. TERMS AND CONDITIONS

- A. *This section establishes the terms and conditions related to Participant Agency responsibilities regarding the provision of data by Data Providers, and the access and use of data by Data Recipients, shared through Worker Connect and any other HHS-Connect applications and infrastructure as specified.***

The undersigned Participants to this Agreement agree to the following terms and conditions:

1. Each Participant shall provide, access, and/or use the data only for permitted purposes consistent with all applicable federal, state and local laws, rules and regulations, and consistent with such participant's participation in HHS-Connect.
2. Each Data Provider shall have sole discretion to determine rights of access to data elements contained within its data source system(s) based upon applicable laws, rules, regulations, and policies. Further, each Data Recipient shall have sole discretion to add additional access restrictions, beyond any imposed by data providers, and based upon applicable laws, rules, regulations, and business policies.
3. Each Participant is responsible for protecting the confidentiality of client information and shall take all reasonable steps to maintain the security of shared data. Further, each Participant is responsible for overseeing the actions of its employees with respect to the provision, use, and access of the data that is shared pursuant to this Agreement.
4. Each Participant agrees that its employees will conduct business consistent with their authorization(s) to participate in HHS-Connect and further agrees to take appropriate disciplinary action where such authorization has been violated and/or misused.
5. Each Participant agrees that all sharing of data shall be in accordance with all applicable laws, rules and regulations, and shall be in furtherance of its programs and/or to advance the common program purpose of Executive Order No. 114.
6. Each Participant is responsible for the maintenance of its own data system.
7. Each Participant will be limited to the modification of only its data. There is no functionality that will permit modification of another Participant's data.
8. Each Participant acknowledges that Participant access and use policies may differ among Participants as a result of differing applicable laws, rules, regulations, and business practices.
9. Agencies providing data make no representations about the accuracy, validity, or authentication of their data.

10. Participants shall immediately remove an Authorized User's access to HHS-Connect if the Authorized User no longer qualifies as an Authorized User due to improper use and/or disclosure.
11. Participants shall immediately remove an Authorized User's access to HHS-Connect if such Authorized User's role and responsibilities change and the user is no longer performing the functions of permitted uses consistent with the agency's participation in HHS-Connect, or the Authorized User is no longer employed by the Participant.
12. Should a Participant request to stop exchanging data with another Participant based upon statutory or regulatory changes, or based on such other Participant's acts in connection with HHS-Connect or this Agreement, the Participant shall immediately notify the HHS-Connect CIO and the ESC of such request and the reasons in support of such request.
13. Inasmuch as this is a multi-party agreement, it avoids the need for Participants to enter into "point-to-point" agreements with each other for the same data and purpose(s) associated with HHS-Connect.
14. Participating agencies shall engage DoITT to automatically revoke access via an automated identity management trigger whenever the NYCAPS system reports that an employee is no longer in active status.

B. In addition to the terms and conditions above set forth for all Participants, each Data Provider and Data Recipient additionally agrees to the following specific set of terms and conditions:

Data Providers

1. The undersigned Participant Data Providers represent and affirm that they have approved all data accessible by Authorized Users through Worker Connect, as of the date of this Agreement, in accordance with all applicable federal, state and local laws, rules and regulations and policies, and that such data may be shared without client consent.
2. Data Providers agree to transmit their data to the CCI and, to the extent consistent with their governing statutes, regulations, rules and policies, to make such data accessible in whole or in part via Worker Connect for use by approved Data Recipients and their Authorized Users for purposes described in business use cases that have been reviewed by Participant Data Providers.
3. Data Providers may exclude certain client data and/or case records based upon applicable laws, rules and/or regulations and policies.
4. Data Providers are expected to maintain their own data, and provide data definitions to HHS-Connect if data will be sourced from them.

Data Recipients

1. No Use by Other than Authorized Users. Data Recipients shall restrict access to HHS-

Connect to Authorized Users and only for authorized purposes (i.e., as described in business use cases approved by Data Providers) consistent with Data Recipients' participation in HHS-Connect.

2. All information accessed as part of HHS-Connect shall be held confidential to the extent required by law, and shall only be used for authorized purposes directly related to the carrying out of Authorized Users' functions and responsibilities consistent with Data Recipient's business use cases and participation in HHS-Connect.
3. Each Data Recipient shall ensure that Authorized Users are trained prior to accessing Worker Connect, understand the guidelines for access and use of confidential data, and train their staff with respect to security and the handling and use of confidential information accessed via HHS-Connect.
4. Each Data Recipient shall use any necessary administrative, technical and physical safeguards to protect the confidentiality, integrity, and availability of information accessed via HHS-Connect.
5. Data shall not be used, without further verification or reconciliation, to determine eligibility for benefits. Absence of data shall not be understood to mean a client is not known to a particular service system. Agencies shall follow their internal verification and case processing procedures for data or discrepancies of data.
6. The Agreement expressly assumes that each City participant will adhere to DoITT's Citywide Users Responsibilities Policy, as well as any additional policies, practices or procedures such Participant has in place regarding the access to and use of City information, including program and client confidential information.
7. Each Data Recipient shall ensure that Authorized Users understand that improper use or disclosure is in violation of the DoITT Citywide User Responsibilities Policy and will result in disciplinary action, and may also subject such employee to civil or criminal penalties.

IV. CONTROLLING LAWS, RULES AND REGULATIONS

Each Participant understands that the provision of, access to, and use of confidential information in connection with HHS-Connect are subject to the laws, rules and regulations of the United States and the State and City of New York.

Change Required to Comply with Applicable Law. Notwithstanding any prior approvals regarding the sharing of information, if a change is required regarding authorized use(s) to comply with statutory and/or regulatory changes, Participants shall notify HHS-Connect CIO and shall work with HHS-Connect Executive Director (a/k/a CIO of Health and Human Services) to implement such change in compliance with all applicable laws, rules and regulations. All Participants shall be notified in the event of a change required to comply with applicable law.

V. IMPROPER USE AND DISCLOSURE

1. Access to HHS-Connect is restricted to Authorized Users.

2. All information accessed as part of HHS-Connect shall be held confidential to the extent required by law, and shall be used by Authorized Users solely for carrying out their functions and responsibilities as Authorized Users directly related to and consistent with Participant Data Recipient's approved business use cases(s).
3. Improper use or disclosure is in violation of the DoITT Citywide User Responsibilities Policy and applicable laws, rules, and regulations.
4. Any individual who has engaged in improper use or disclosure of HHS-Connect information will be subject to his or her agency's disciplinary process.
5. Any individual who has engaged in improper use or disclosure of HHS-Connect information may be subject to civil and/or criminal penalties.
6. Participants shall immediately remove an Authorized User's access to HHS-Connect if the Authorized User has engaged in improper use and/or disclosure.
7. Required Notice to Data Providers: Should data obtained from Worker Connect be improperly released (e.g., misplaced or stolen, or disclosed in an unauthorized manner) or where the Data Recipient discovers evidence of willful or intentional misuse of data, the Data Recipient shall inform the Data Provider whose information has been improperly released or misused within 72 hours of discovery by the Data Recipient.

VI. DISCLAIMERS

Reliance on a Data Source System: Nothing in this Agreement shall be deemed to impose responsibility or liability on a Participant related to the accuracy, content or completeness of any data provided pursuant to this Agreement. The Participants acknowledge that other Participants may be added or terminated as participants in HHS-Connect at any time; therefore, Participants may not rely upon the continued availability of a particular Participant's data.

VII. SECURITY

Pursuant to Executive Order No. 114, HHS-Connect was developed in alignment with the security requirements and enterprise architecture standards as set forth by the Department of Information Technology and Telecommunications (DoITT). Multiple technologies have been deployed with data protection capabilities, including: 1) access controls; 2) field by field redaction; 3) upstream and downstream filtering; 4) encryption; 5) filtering logic to restrict quantity of data provided; and 6) auditing. The Access Management system provides policy-based authentication and authorization of users. Access is obtained only by individuals whose credentials are verified upon Log-In against the DoITT managed enterprise LDAP directory and have been approved by their agency. The system filters data based upon Authorized Users assigned role and agency. Worker Connect activities will be recorded in security audit logs. All use will be subject to compliance with the published Citywide Information Security Policies and standards which can be reviewed at <http://cityshare.nycnet/infosec>.

VIII. SEVERABILITY

The provisions of this Agreement are severable. If any provision of this Agreement is held invalid by any court that invalidity shall not affect the other provisions of this Agreement and the invalid provision(s) shall be considered modified to conform to the existing law.

IX. ADDITIONAL PARTICIPANTS

The undersigned Participants acknowledge that additional Participants (Data Providers and/or Data Recipients) may be added to HHS-Connect. All current Participants agree that, prior to admission of a new HHS-Connect Participant, the new Participant must agree to be bound by the terms of this Agreement. An additional Participant, if not a current signatory, shall stipulate to all the terms of this Agreement. The Participants agree that upon such stipulation by a duly authorized representative of such additional Participant, such additional Participant shall be deemed to be a signatory to this Agreement and will be bound by all the terms of this Agreement.

X. EFFECTIVE DATE

This Agreement shall remain in full force and effect immediately from the date of execution.

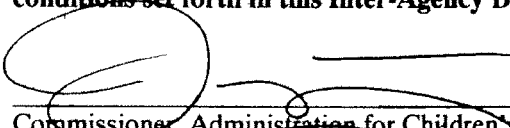
XI. MODIFICATION / TERMINATION

This Agreement may only be modified or terminated in writing by mutual consent of all Participants.

XII. ENTIRE AGREEMENT

This written Agreement contains all the terms and conditions agreed upon by the parties hereto. The terms and conditions of this Agreement constitute the full and complete agreement between the Agencies. No other verbal agreement shall, in any way, vary or alter any provision of this Agreement. No other written agreement shall, in any way, vary or alter any provision of this Agreement unless modified in writing by mutual consent of all Participants or as required by statutory or regulatory changes.

The undersigned hereby accept and agree to be bound by all of the provisions and terms and conditions set forth in this Inter-Agency Data Exchange Agreement.



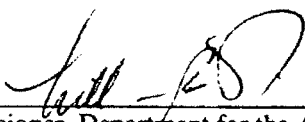
Commissioner, Administration for Children's Services/
Commissioner, Department of Juvenile Justice

11/5/10
Date



Commissioner, Human Resources Administration

11/8/10
Date



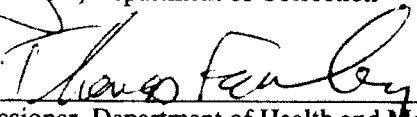
Commissioner, Department for the Aging

11/5/10
Date



Commissioner, Department of Correction

11/8/10
Date




Commissioner, Department of Health and Mental Hygiene

11/12/10
Date




Commissioner, Department of Homeless Services

11/5/10
Date




Commissioner, Department of Probation

11/12/10
Date



President, Health and Hospitals Corporation

11/12/10
Date



Commissioner, Department of Information Technology
& Telecommunications

12/3/10
Date



Chairman New York City Housing Authority

11-29-10
Date



Commissioner, Department of Finance

11-29-10
Date

Attachment A



THE CITY OF NEW YORK
OFFICE OF THE MAYOR
NEW YORK, N.Y. 10007

EXECUTIVE ORDER No.114

HHS-CONNECT

March 18, 2008

WHEREAS, this Administration is committed to improving the delivery of services to New Yorkers with state-of-the-art technology; and

WHEREAS, the City provides a wide range of health and human services to a diverse client population; and

WHEREAS, among the agencies providing such services are the Administration for Children's Services, Department for the Aging, Department of Correction, Department of Health and Mental Hygiene, Department of Homeless Services, Department of Juvenile Justice, Department of Probation, Health and Hospitals Corporation, and Human Resources Administration, referred to collectively herein as "HHS agencies;" and

WHEREAS, many New Yorkers qualify for and participate in multiple programs provided by different HHS agencies; and

WHEREAS, sharing of client data among HHS Agencies will provide a more complete understanding of clients' needs and enable more efficient and effective service delivery; and

WHEREAS, the City has committed to launching HHS-Connect, a technology solution that connects clients, agencies, and providers, and will utilize ground-breaking and innovative technologies to improve the City's ability to serve its population;

NOW, THEREFORE, by the power vested in me as the Mayor of the City of New York it is hereby ordered:

Section 1. HHS-Connect is hereby established to facilitate data integration and exchange between existing agency-based information management systems through the following:

- a. Innovative technology tools. HHS-Connect shall implement innovative tools to provide City workers with cutting-edge technologies to improve the speed and accuracy of services.

- b. Common data model. HHS-Connect shall support data integration and exchange, including creation of a common data model for HHS-Connect.
- c. Data sharing strategy. HHS-Connect shall employ a data sharing strategy to enable relevant agencies to exchange client and program data.
- d. Enterprise case management. HHS-Connect shall provide requesting HHS agencies with a common technology platform for case management.
- e. Integrated case folder. HHS-Connect shall oversee the creation of a virtual integrated case file for clients, using a common client index to locate clients in separate systems and document image management tools to electronically capture and share client documents. This case folder shall be available online.
- f. Business process reengineering. HHS-Connect shall ensure streamlined business processes to improve and coordinate case management practices across agencies.
- g. Performance measurement and outcome evaluation. HHS-Connect shall enable the City to measure client outcomes based on a holistic view of clients across agencies.
- h. Confidentiality. HHS-Connect shall ensure the protection of the confidentiality of information as required by applicable law.

§2. All agencies are directed to identify appropriate programs, data and technology assets that can expand and enhance HHS-Connect. To the greatest possible extent, HHS-Connect shall leverage existing Citywide technology assets to accelerate the pace of the project and increase the effectiveness and efficiency of the services delivered to the Agencies, their clients, and external service providers.

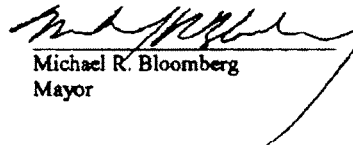
§ 3. Data Sharing. For the purposes of HHS-Connect, agencies shall consider all data for data sharing while ensuring compliance with all applicable Federal, State and local laws and regulations. To facilitate data sharing, agencies shall work with the HHS-Connect team to identify data sharing needs, as well as sources and types of data. Data sharing shall occur in a timely fashion and agencies shall facilitate real-time data exchanges whenever possible, as set forth by the HHS-Connect data sharing strategy.

§ 4. Alignment with Citywide IT Strategy. HHS-Connect shall be aligned with and further the Citywide Information Technology strategy, including security requirements and enterprise architecture standards, as set forth by the Department of Information Technology and Telecommunications ("DOITT").

§ 5. HHS-Connect shall be implemented by a Chief Information Officer for Health and Human Services ("CIO for HHS") who shall report to the Deputy Mayor for Health and Human Services, or other appropriate senior level official, and shall provide oversight and coordination of the technology strategy and architecture of HHS agencies, in conjunction with DOITT.

§6. Cooperation and Assistance: The heads of all agencies shall cooperate with and assist the CIO for HHS in the implementation of HHS-Connect as requested.

§7. This Order shall take effect immediately.



Michael R. Bloomberg
Mayor

Stipulation and Agreement of Terms for New Member Agencies and Users of Worker Connect, a
New York City Application Administered by HHS Connect

Whereas, in support of Executive Order No. 114, the Inter-Agency Data Exchange Agreement, executed in November of 2010, (the "Agreement"), sets forth a common set of terms and conditions in support of a secure interoperable data exchange between and among health and human services agencies and related agencies.

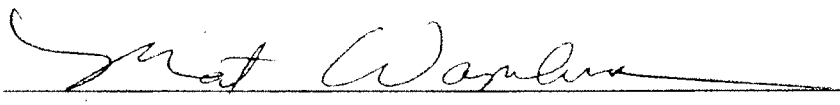
Whereas, the undersigned agencies have agreed to receive and/or provide data from the named data source systems and have jointly, with HHS Connect, established applications and infrastructure with which to share data to improve services to citizens of New York City.

Whereas, the undersigned agencies recognized that many New Yorkers qualify for and participate in multiple City programs. Leveraging advances in modern technology will break down information silos and:

- Improve client outcomes
- Increase the reliability of data
- Reduce duplication of client data
- Improve integration of client services
- Promote a client-centric approach to service delivery
- Improve accessibility and management of information
- Improve program effectiveness, performance, and accountability.

Whereas, the proposed member agency, the New York City Department of Housing Preservation and Development (HPD) has determined that its programs and operations would benefit from participating in this Agreement,

Now, therefore, pursuant to Section IX of the Agreement, HPD is added as an "additional participant." HPD hereby accepts and agrees to be bound by all of the provisions and terms and conditions set forth in the Agreement.

 2/15/13

Matthew M. Wambua,
Commissioner, Department of Housing Preservation and Development

Date

Jefferson County, Colorado Memorandum of Understanding

**MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451**

This Agreement is made by and between the **JEFFERSON COUNTY DEPARTMENT OF HUMAN SERVICES (“Social Services”)**, located at 900 Jefferson County Parkway, Golden, Colorado 80401; the **FIRST JUDICIAL DISTRICT PROBATION DEPARTMENT (“Probation”) AND THE FIRST JUDICIAL DISTRICT (“Judicial”)** located at 100 Jefferson County Parkway, Golden, Colorado 80401; the **JEFFERSON COUNTY DEPARTMENT OF HEALTH AND ENVIRONMENT (“Health”)**, located at 1801 19th Street, Golden, Co. 80401, the **JEFFERSON COUNTY SCHOOL DISTRICT, (“School District”)**, located at 1829 Denver West Drive, Building 27, Golden, Co. 80401; the **JEFFERSON CENTER FOR MENTAL HEALTH, (“Mental Health”) a non-profit corporation whose principal place of business is located at 4851 Independence Street, Wheat Ridge, Co. 80033** and **FOOTHILLS BEHAVIORAL HEALTH, LLC (“BHO”)** located at 9101 Harlan Street, Suite 100, Westminster, Co. 80031, the **DIVISION OF YOUTH CORRECTIONS (DYC)** located at 4255 S. Knox Court, Denver, Co, the **DEVELOPMENTAL DISABILITIES RESOURCE CENTER (DDRC)** located at 11177 West 8th Avenue, Suite 300, Lakewood, Co. 80215 and the **JEFFERSON COUNTY AFFILIATE OF THE FEDERATION OF FAMILIES FOR CHILDREN’S MENTAL HEALTH, COLORADO CHAPTER IN PARTNERSHIP WITH THE JEFFERSON COUNTY FAMILY SUPPORT NETWORK (JFSN)** located in Wheat Ridge, Colorado. Each signatory to this agreement is referred to as a “Party”, and collectively as “Parties”.

WHEREAS, the Colorado General Assembly has determined that a collaborative approach to the delivery of services to children and families may lead to the provision of more appropriate and effective delivery of services; and

WHEREAS, the Colorado General Assembly has determined that such collaboration may ultimately allow the agencies providing treatment and services to provide appropriate services to children and families within existing consolidated resources; and

WHEREAS, the Colorado General Assembly has determined that it is in the best interests of the State of Colorado to establish a collaborative management of multi-agency services provided to children and families; and

WHEREAS, Colorado revised statutes, Section 24-1.9-101, et.seq. authorizes the county department of social services to enter memorandums of understanding with specific agencies for the purpose of promoting a collaborative system of local-level interagency oversight groups and individualized service and support teams to coordinate and manage the provision of services to children and families who would benefit from integrated multi-agency services; and

WHEREAS, the undersigned desire to enter into an agreement for the collaboration of services to families and children who would benefit from integrated multi-agency services; and

WHEREAS, the undersigned agencies include all of the agencies required by statute;

NOW THEREFORE, in consideration of the premises and mutual promises and covenants herein contained, the Parties agree as follows:

The Agreement. This Memorandum of Understanding (“MOU” or “Agreement”) is contained in this writing, which consists of 36 pages.

Term of the Agreement. This MOU shall be effective beginning July 1, 2007 and shall expire June 30, 2008.

I. Renewal of MOU. The Parties may renew this MOU annually subject to mutual agreement. Each Party reserves the right to elect not to renew the MOU after expiration of the current term. If any Party intends not to renew the MOU, it shall give notice of such intent at least thirty (30) days prior to expiration of the Agreement.

II. Population to be Served. The persons who will be recipients of services under this MOU shall be “children and families who would benefit from integrated multi-agency services”, (“Recipients”). This population of children and families is defined as follows:

Families and their children who meet the eligibility criteria for one of the Child Welfare Program areas 4, 5, or 6 as defined in the Colorado “Policy and Procedures for Child Welfare services” manual, Volume VII, and

Who are involved with at least one other participating agency to this MOU in addition to Child Welfare, and

Who are at risk of or are currently in out of home placement, psychiatric or medical hospitalization, and/or who are at risk of delinquency or commitment to the Department of Youth Corrections.

Jefferson County estimates it will serve at least 70% of its Child Welfare caseload or approximately 1590 children.

III. Services and Funding Sources. The Parties agree to provide the following specific services and subject to available funds, hereby identify the following funding sources for the provision of such services.

A. Social Services:

1. Goal(s):

The Mission of the Children, Youth and Families Division is to promote the safety, well-being, and permanency of children and youth.

The Mission of the Systems of Care grant is to promote the welfare of children and families through the development of sustainable partnerships that provide integrated, quality services that are individualized, strength-based, family centered and culturally competent.

The goals for the Child Welfare program area 4, Youth in Conflict, are alleviating conflicts and protecting the youth and the community, reestablishing family stability, and assisting the youth to emancipate successfully.

The goals for the Child Welfare program area 5, Children in Need of Protection, are that children are secure and protected from harm, have stable, permanent and nurturing living environments, and when appropriate, experience family continuity and community connectedness.

The goals for the Child Welfare program area 6, Children in Need of Specialized Services, are to fulfill statutory requirements in the interests of permanency planning for children.

2. Services to be contributed to this project and amounts associated with those services:

Jefferson County is developing and implementing a Systems of Care (SOC) model. SOC is a continuum of services organized into a coordinated network to meet the needs of children and families. It is based on the principles of interagency and community collaboration, individualized, strength and community based services, cultural competency, family involvement and accountability.

CYF is utilizing Team Decision Making, a Family to Family strategy to enhance family and community involvement in case planning, and CYF is performing utilization management through “Options” staffings which bring together CYF, agency partners, and families to develop alternatives to highly restrictive levels of care.

CYF has developed an early intervention team to enhance our voluntary services for families and to reduce our reliance on legal interventions and out of home placements.

CYF will be responsible for:

- Active participation in the Interagency Oversight Group as a voting member.

- Leadership and staff support through CYF and SOC for the development of the Collaborative Management (CM) Memorandum of Understanding (MOU) and for the CM IOG.

- At least 70% of all Services provided to the Target Population through CYF staff and contracts which include Intake, Early Intervention Services, Ongoing Youth and Child Protection Services, Resource Development Services, Adoption Services, Core Services, Day Treatment, Home Based Services, Intensive Family Therapy, Mental Health Services, Sex Abuse Treatment Services, Substance Abuse Treatment Services, Life Skills Services and Special Economic Assistance Program.

- At least 70% of the SOC grant

3. Staff who will contribute to those services and amounts associated with those staff:

The SOC staff are the Program Manager, Parent Partner Coordinator, Training Coordinator, Administrative Specialist, Volunteer Coordinator and research provided by the Butler Institute at the University of Denver.

CYF offers the following staff to participate in the implementation of this MOU in collaboration with the co-signers and the community at least 70% of their time to at least 70% of the population served:

Division Director (1 FTE)
Program Managers (4 FTE)
Supervisors (20 FTE)
Caseworkers (110 FTE)
Case Aides (9 FTE)
Support Staff (6 FTE)
Financial/Billing/Payroll Staff (11 FTE)

4. Funding sources

A. Federal Grants:

\$347,924 of federal funds for 70% of the Systems of Care Health and Human Services Grant*

B. Child Welfare Block Grant Allocation:

Total Block Allocation = \$27,684,240 (includes county money of \$4,334,213)
70% of Total Block Allocation = \$19,378,968 for CM

C. Core Services Allocation:

Total Core Services Allocation=\$3,867,203
70% of Total Core Services Allocation=\$2,707,042 for CM

* The SOC grant is subject to renewal each Federal fiscal year.

The Child Welfare Block Grant and the Core Services Allocation will change on July 1, 2008; therefore these figures will need to be revised at that time to reflect these numbers.

B. Probation:

1. Goals:

Probation Mission Statement: Colorado Probation is Committed to Public Safety, Victim and Community Reparation through Offender Accountability, Skill and Competency Development and Services to the Communities of Colorado.

As such, the goals include:

Complete Predispositional Reports as required by the court.

Supervise all adult and juvenile offenders ordered to complete probation, assisting them to develop skills and thinking that will help them to remain in the community, reduce recidivism, and reduce their risk to the community and themselves. This is done effectively by case planning that includes assessment services, referral services, supervision, and detainment, when necessary.

Restore the community, victims, and the offender, insuring that any harm created by the offender is addressed and reparations made where appropriate.

Follow all tenants of the Victim Rights Amendments, including notification of status changes in their case.

2. Services to be contributed to this project and amounts associated with those services:

Active participation in the IOG as a voting member. **Staff time estimated \$4,000**

Probation will be responsible for providing probation supervision services for all juvenile and adult offenders sentenced to probation, including cases of Deferred Adjudications and Informal Adjustments, as is the case with the proposed 1st Judicial District Juvenile Mental Health Court.

Drug and Alcohol Assessment Services will be provided, with priority to in-custody juveniles (.75 FTE – SB94). Also on adult offenders a SSI and 1173 assessment will be completed. **Staff time estimated \$3,000**

Juvenile Education Program (JEP) provided for juveniles that are expelled or suspended, with priority given to those youth that are under the age of 16. Contained classroom with individualized instruction (.50 FTE – SB94). **Staff time estimated \$16,000**

Drug/Alcohol outpatient treatment funding provided through probation's Offender Services Fund. Limited to juvenile and adult offenders in financial need. Also RIS – "Rapid Intervention Services fund (SB94) – probation has referral access to these funds for Drug/Alcohol treatment and family and individual counseling for clients that have financial need for assistance in paying for outpatient treatment. **(See below)**

Sex Offender Psycho-Social Evaluations – probation fund assists probation officers working jointly with CYF caseworkers to pay for intensive evaluations to determine risk and level of treatment needed for sexually abusive youth. **(See below)**

Cognitive/Behavior groups – "Thinking for a Change." These closed groups are led by probation officers in the 1st Judicial District. **Staff time estimated \$2000**

Victim empathy groups – Facilitated by probation officers to increase victim awareness and empathy among juvenile and adult offenders. **Staff time estimated \$1500**

Jefferson County Community Restorative Justice Program – will be available to any juvenile or adult offenders, families, victims or community groups that would benefit from conferencing circles. (.50 FTE) **Staff time estimated \$2,000**

JISP – Juvenile Intensive Supervised Probation. Provided for juveniles at risk of placement in a human services contracted treatment facility, or detention. (2.5 FTE).

Staff time estimated \$10,000

3. Staff who will contribute to those services and amounts associated with those staff:

All juvenile probation officers and juvenile supervisors in the 1st Judicial District will work with other agency personnel as needed to comply with the terms of this MOU. Funding is provided by the State of Colorado through the Judicial Department to support these services (15.0 FTE).

Additionally, as needed, all adult probation officers and adult probation supervisors will work with other agency personnel to be in compliance with this MOU. These positions are funded by the State of Colorado State Judicial and represent 55 FTE to include probation officers, VACs, CIs, and management staff.

4. In-kind contributions and the amounts associated to those contributions:

Probation supervisor and designees will participate in planning and ongoing facilitation of IOG meetings, facility space in Courthouse for meetings, Emergency Release staffings, DYC staffings, Options staffings, Team Decision-Making Meetings and other meetings related to the MOU.

Staff time estimated \$6000

5. Funding sources

Offender Services Funds (probation) – State Judicial	<u>\$10,000</u>
Offender Services Funds earmarked for Juv Sex offender evaluations	<u>\$2100</u>
Probation Department FTE staff time– State Judicial (from above)	<u>\$30,500</u>
RIS – (Rapid intervention Services) through SB94	<u>\$5000</u>
SB94 FTE dedicated to probation programming/services.	<u>\$3000</u>
Total	<u>\$50,600</u>

C. Health:

1. Goals:

The mission of Jefferson County Department of Health and Environment (JCDHE) is to create, promote and enhance health and vitality through innovation, collaboration and celebration. JCDHE meets this goal through its four divisions: Administrative, Community Health Services, Environmental Health Services, and Health Promotion and Lifestyle Management.

2. Services to be contributed to this project and amounts associated with those services:

Participating in the Jefferson County Interagency Oversight Group (IOG) as a voting member.

Providing information and referral to programs in the community and at JCDHE. Based on requirements of the target population and referral for service, JCDHE services may include:

Health Care Program for Children with Special Needs (HCP) including traumatic brain injury

Family planning and reproductive counseling

Health care access assistance for CHP+, Medicaid and EPSDT

Immunizations

Women, Infant, and Children Federal Nutrition Program

Drug and alcohol counseling and prevention

Nurse home visits including Expedited Permanency Planning placements

Sexually transmitted diseases diagnosis and treatment

HIV counseling and testing

Epidemiologic surveillance

Birth and death certificates

Environmental assessments

3. Staff who will contribute to those services and amounts associated with those staff:

The Director of the JCDHE Community Health Services Division, or her alternate, will attend required meetings.

4. In-kind contributions and the amounts associated to those contributions:

In-Kind Contributions:

IOG staff time

IOG lunches

Options staff time

Core Services Advisory staff time

Core Services Expedited Permanency Planning (maximum of \$20,000)

Child Protection Team staff time

JCDHE services as listed (not included in estimated in-kind)

Estimated in-kind: \$35,300

JCDHE supports the target population through in-kind services of staff including attendance at Options staffings by the Drug and Alcohol Liaison, and participation in the Core Services Commission and the Child Protection Team.

5. Funding sources

Funding Sources:

State and Federal grants

Private Foundation grants

Client fees

Client donations

Medicaid

Third party insurance
Core Services allocation (maximum of \$20,000)
Contracts
Per capita monies
County monies

Due to the numerous funding sources for services at the Department of Health, it is difficult to break all the funding amounts out for each service since it is difficult to calculate the number of referrals that will be made to programs or the number of children seen in each program who are also enrolled in child welfare services.

D. Schools:

1. Goals:

Jefferson County Public Schools mission: “To provide a quality education that prepares all children for a successful future.”

2. Services to be contributed

Active district administrative staff participation in IOG meetings as a voting member

Student health care planning and support during the school day as provided by district nursing staff and designated school staff

Student and family health care enrollment assistance through school Medicaid and CHP+ outreach program

District administrative liaison support and participation on the Jefferson County Child Protection Team

Consultation and collaboration with community agencies during risk assessments and student transitions

Coordination and implementation of Individual Education Plans for Special Education Students

District collaboration and participation as appropriate and requested in Jeffco Options meetings and Core Service Commission

Utilize understanding of HB 04-1451 to study and build capacity in a Systems of Care Model and collaborative management process to promote welfare of children.

3. Funding Sources

In-kind contributions

- School district will continue to provide central administrative support for participation in the IOG.

- The School District is unable to estimate the actual amount of these contributions due to the change in the educational outcome measure. Without at least one year's operational figures regarding the number of youth being served by the Jefferson County School District and Jefferson County Division of Children, Youth and Families who are eligible for services through this MOU, it is difficult to calculate actual cost.

School District Profile

Elementary Schools	93
Middle Schools	18
High Schools	17
Option Schools	7
Charter Schools	12

Student Enrollment	85,478
--------------------	--------

American Indian/Alaska Native	1.13%
Asian or Pacific Islander	3.57%
Black	1.94%
Hispanic	16.43%
White	76.93%

Where the School Districts Funding Comes From

49% State of Colorado

42% Property Tax

5% Automobile Ownership Tax

4% Other (interest, tuition and fees)

Where the Funding Goes

Schools 88.1%

Business Expenses 3.9%

School Support 8%

Total Revenue: \$596.1 million

(2004-2005, Annual Report)

E. Mental Health:

1. Goals:

The mission of Jefferson Center for Mental Health is to promote, support and improve the mental health of the community, and provide quality mental health services to persons with emotional problems and/or serious mental illness. The Center's shared values include: Serve our customers with respect. Provide quality treatment options and empowerment opportunities for consumers. Strive for mutual respect, collaborative relationships, individual accountability, and successful outcomes. Accept individual empowerment and the responsibility for high achievement. Trust and respect one another. Be creative and flexible as we go about helping others while thoughtfully protecting their personal dignity.

2. Services to be contributed to this project and amounts associated with those services (contingent on availability of resources, and for youth and/or family members meeting medical necessity criteria):

Jefferson Center for Mental Health will be responsible for:

Active participation in the IOG as a voting member

Provide community-based mental health services for youth ages 0-18 (up to age 22 for youth attending The ROAD) and their families living in Jefferson County.

These services shall include: mental health assessment/evaluations, group, family, individual, and play therapy, case management, medication evaluation and follow-up

appointments, and mental health emergency services available 24 hours a day/ 7 days a week. The Center also offers specialized evidence based, promising and innovative practices such as Functional Family Therapy, Multi-systemic Therapy, Dialectical Behavior Therapy, Cognitive Behavioral Therapy, Trauma Treatment, Wraparound, school-based counseling, home-based family treatment, transition services for youth aged 15-22 at The ROAD and Cross Roads program (for youth referred by Probation, SB-94 and the JAC).

Staff who will contribute to those services and amounts associated with those staff:

Jefferson Center for Mental Health has approximately 300 staff - including psychiatrists, psychologists, psychiatric nurses, licensed clinical social workers and professional counselors, case managers and vocational counselors. It also has access to a comprehensive network of external providers for Medicaid recipients through its association with Foothills Behavioral Health. Jefferson Center's Deputy Chief Operating Officer and /or Family Services Manager will participate in the IOG meetings.

3. In-kind contributions and the amounts associated to those contributions:

IOG staff time	\$ 500
Options staff time	2795
Team Decision-Making staff time	2,078
Core Services Advisory staff time	401
Child Protection Team staff time	1748

Case management/wraparound for non-Core funded CYF target population clients	15945
Management (CYF/JCMH) meetings- case staffings and system issue resolution	2135

Estimated total in-kind:	\$25,602
--------------------------	----------

4. Funding sources

Core Services
Jefferson County Contract for children with no payor source
Medicaid
Grants
Client fees
Third party (insurance)
Division of Mental Health

F. Behavioral Health:

1. Goals:

Foothills Behavioral Health (FBH) is the designated Behavioral Health Organization (BHO) for Jefferson, Clear Creek, Gilpin, Boulder and Broomfield Counties. Our mission is to arrange access to and reimburse for the provision of medically necessary mental health services for individuals who are Medicaid eligible in the five county area. These services are provided by our two Network Mental Health Centers (i.e., Jefferson Center for Mental Health and the Mental Health Center Serving Boulder and Broomfield Counties) and our Independent Provider Network consisting of individual and organizational providers across the five county area. The two Network Mental Health Centers generally serve as the frontline access point for the majority of individuals seeking Medicaid funded mental health services and work closely with FBH to maintain standards of quality and service access.

2. Services to be contributed to this project and amounts associated with those Services:

A member of the FBH staff and an alternate will be designated as active participants in the planning and implementation phases as well as a voting member(s) of the IOG.

3. Staff who will contribute to those services and amounts associated with those staff:

FBH, as an organization, will use all necessary staff resources to ensure that authorized and medically necessary mental health services are provided to members of its health plan who are participants in the collaborative management program.

4. In-kind contributions and the amounts associated to those contributions:

FBH estimates that in-kind contributions tied to staff time and travel expenses for IOG meetings will be \$4,650.

5. Funding sources:

FBH receives its funding through the Colorado Medicaid Community Mental Health Services Program under contract with the Department of Healthcare Policy and Financing. These funds, currently estimated at \$25 million for the five county area are restricted to the purchase of medically necessary mental health services for individuals who are eligible for Medicaid and members of FBH's health plan.

G. Division of Youth Corrections and SB 94:

1. Goal:

The Division of Youth Corrections (DYC) and SB 94 are committed to enhancing public safety by partnering with local agencies and citizens to build better service capacity in

assessment, case planning, treatment, and continuing care for at-risk youth in those communities.

2. Services and Staff to be Contributed:

In order to fulfill that commitment NYC and SB 94 agree to the following as our investment in this MOU.

- NYC and SB 94 will continue to provide management level staff time to participate in the IOG for this MOU.
Assistant Director (4 hours/month)
SB 94 Coordinator (4 hours/month)
Total: \$3230
- NYC will provide space at Montview Detention Center for multidisciplinary screenings, which may include family members and/or family advocates, designed to provide better sentencing recommendations and pretrial release planning.
Facility Meeting Space Undetermined at this time
- NYC and SB 94 will be actively involved in those screenings and will share their expertise to provide for higher quality assessments.
Client Managers (2 hours/week) \$2500
Client Manager Supervisor (4 hours/week) \$6000
SB 94 Coordinator (6 hours/week) \$10,500
- NYC and SB 94 will continue to be involved in the collaborative management of SB 94 services and resources at the local level.
SB 94 Annual Budget*
- NYC will work collaboratively with local entities and families in the transition of youth as they parole back to their home communities.
Residential Purchase of Services*
Continuum of Care Services*
- NYC will also participate with county agencies in the development of juvenile justice initiatives in those local communities.

*Unable to determine amount of contribution without at least one year's operational figures regarding how many youth NYC and SB 94 served are also a part of the child welfare target population

H. Court:

The First Judicial Courts support the implementation of HB 1451 through necessary in-kind services of judicial and non-judicial staff. Approximate in-kind contribution is \$3,000.

I. Developmental Disabilities Resource Center:

1. Goals of agency:

Developmental Disabilities Resource Center (DDRC) Mission Statement:

- The mission of Developmental Disabilities Resource Center (DDRC) is to provide leading edge services that create opportunities for people with developmental disabilities and their families to participate fully in the community.

DDRC Vision Statements:

- DDRC will be known for providing easy access to customer-centered, quality services.
- DDRC will be recognized locally and nationally as a leader in providing a quality work environment for all employees.
- DDRC will expand partnerships with the people we serve, providers, advocates, and community resources so services are an integral part of our communities.
- DDRC will help people of Colorado accept people with disabilities and welcome them in every part of community life.

DDRC Values:

- Quality, dignity and choice.

DDRC is the Community Centered Board (CCB) for Jefferson, Clear Creek, Gilpin and Summit Counties. CCBs are nonprofit organizations contracted with by Colorado Department of Human Services, Division for Developmental Disabilities (DDD) to manage resources at the local level, to determine eligibility for community based services and provide case management services. The 20 community centered boards in Colorado are designated by the State and may either provide child and adult services directly or purchase services.

There is no entitlement to funding or services within the developmental disabilities system; therefore not everyone who is eligible for services receives services. There are waiting lists for services.

Eligibility Criteria

In Colorado, a **developmental disability** is defined as a disability that:

- ✓ Occurs before the person reaches 22 years of age,
- ✓ Substantially impacts the person's daily life,
- ✓ Is caused by mental retardation or related conditions...for example – cerebral palsy, autism, epilepsy, Down Syndrome, or other neurological conditions, and
- ✓ Impairs the person's general intellectual functioning: IQ 70 or below,
- ✓ Significantly limits daily living skills in 2 or more areas.

A **developmental delay** refers to the slowed or impaired development of a child who meets one or more of the following criteria:

- (1) children less than five years of age who experience a delay in one or more of the following areas:
 - a) physical or motor (moving);
 - b) communication (babbling/talking);
 - c) sensory (hearing/seeing);
 - d) cognition (learning);
 - e) social/emotional (playing and interacting);

f) adaptive development (self help skills).

(2) children less than five years of age who are at risk of a developmental disability because of the presence of chromosomal conditions, congenital syndromes, metabolic disorders, prenatal and perinatal infections, postnatal conditions affecting development, or low birth weight.

(3) children less than three years of age whose parents have a developmental disability.

DDRC CHILDREN AND FAMILY SERVICES

CASE MANAGEMENT/ RESOURCE COORDINATION

Case managers (also known as Service or Resource Coordinators) are qualified professionals trained to help people with developmental disabilities- and their families – navigate all the different types of services that may be available to meet the person’s needs. Case managers work at Community Centered Boards and provide a variety of case management activities, such as:

- Determining eligibility for services
- Describing services and how to apply
- Helping determine needs
- Working together with the person and others to develop an individualized plan
- Providing ongoing monitoring and coordination of services

EARLY INTERVENTION SERVICES (EI)

As part of Early Childhood Connections in Jefferson, Clear Creek, Gilpin and Summit Counties, DDRC offers educational and therapeutic supports to children birth to three with developmental concerns. Early intervention services are designed to enhance the capacity of families to support their children’s well being, development, learning, and full participation in their communities. Services address desired functional outcomes and are provided in families’ everyday routines, activities and places.

FAMILY SUPPORT SERVICES PROGRAM (FSSP)

Family Support is intended to support families who have children with developmental disabilities or delays with costs that are beyond those normally experienced by other families. The primary purpose of the FSSP is to support children with developmental disabilities or delays remain within their own nurturing family setting and prevent out-of-home placements. FSSP offers both money and Resource Coordination. It is a state-funded program and is not income based. In order to receive funding families must complete a Needs Assessment and be determined most-in-need of State Family Support funds relative to other families- based on five parameters: Overall care needs, behavior, family composition and stability, access to support networks, and access to other resources. Services that can be paid for using FSSP funds include, but are not limited to:

- **Respite Care:** The temporary care of a person with a developmental disability in order to offer relief to the person’s family or caregiver, to allow the family to deal with emergency situations, or to engage in personal, social activities.

- **Professional Services:** Therapy, individual counseling, behavioral intervention, consultation or other services provided by an appropriately qualified person or agency to the family member with a developmental disability.
- **Medical and Dental:** Medical and dental expenses for a family member with a developmental disability not covered by health insurance or other programs. Examples include co-pays, syringes, feeding tubes, suctioning equipment, catheters, lodging and food expenses incurred during out of town medical treatment, or long distance calls to arrange or coordinate medical services.
- **Transportation:** Transportation costs related to providing care and support to a family member with a developmental disability which are above and beyond those typically incurred by other families. Mileage to medical, therapy or program appointments not covered by other sources can be reimbursed at .405 per mile.
- **Other Individual Expenses:** Services or items which are provided for the person with a developmental disability which are necessary as a result of the person's disability, including physical, medical, educational or behavioral needs. Examples: diapers for a child age 3 or older, special diets, specialized clothing, and developmental toys and materials.
- **Assistive Technology:** Any equipment that pertains directly to supporting the individual with a developmental disability in the home. Examples include *mobility aids* such as wheelchairs, strollers, orthotics, braces; *adaptive equipment* such as special beds, switches, tools or jigs; *communication devices*, *glasses*, *hearing aids*, *special kitchen appliances*, or *vehicle modifications* to enable access by the family member with a developmental disability.
- **Home Modifications:** Physical adaptations to the home environment such as ramps, lifts, widened doorways, accessible bathrooms. Repair of home structure or replacement of items damaged by the eligible family member due to aggressive behavior, not normal wear and tear.
- **Parent and Sibling Support:** Activities to reduce stress related to caring for a family member with a developmental disability such as homemaker services, recreation and leisure activities, costs of memberships in support organizations, family counseling, special resource materials or publications, genetic counseling, behavioral intervention or training; and sitter care for siblings while the person with a disability is taken to medical or therapy appointments.

FAMILY SUPPORT LOAN FUND

The purpose of the Family Support Loan Fund is to provide access to short-term low interest rate loans in order to obtain family support services, which help to maintain a dependent family member with a developmental disability in the home. Applications are accepted by the Division for developmental disabilities (DDD) during the open application period, January 1, through February 15. Maximum loan amount \$8000, maximum repayment period 60 months, Colorado State Treasurer calculates the interest

rate based on the annual earning rate for the preceding fiscal year (for loans made in 2006 it will be 3.18%). Allowable purchases are similar to those listed above for FSSP.

CHILDREN'S MEDICAID WAIVER PROGRAMS (C-HCBS, CES)

The Children's Home and Community Based Services Waiver (C-HCBS), and the Children's Extensive Support Waiver (CES) are Medicaid Waiver Programs for children birth through 17 who meet specific eligibility criteria. To qualify for Medicaid long-term care services, the child must have deficits in two of six Activities of Daily Living (bathing, dressing, toileting, eating, mobility and transferring), or require supervision due to a behavior or memory/cognition deficit.

- **C-HCBS (administered by Health care Policy and Financing)** provides Medicaid benefits to children who are at risk of hospitalization or nursing home placement. Children who have significant personal care, therapy, and/or medical needs may qualify. Applicants must be *ineligible* for Supplemental Security Income (SSI) due to excess parental income. Families may apply for this program through their local Community Centered Board (e.g., DDRC), County Human Services office, or any other Case Management Agency.
- **CES** provides Medicaid- funded services and supports to children with developmental disabilities or delays who have the most intensive behavioral and/or medical needs and are at high risk of out-of-home placement. Eligible children demonstrate a behavior or have a medical condition that requires direct human intervention, more intense than a verbal reminder, re-direction or brief observation of medical status, at least once every two hours during the day and on a weekly average of once every three hours during the night. The behavior or medical condition must be considered beyond what is typically age appropriate and be due to one or more of the following conditions:
 - (a) A significant pattern of self-endangering behavior(s) or medical condition which, without intervention will result in a life threatening condition/situation.
 - (b) A significant pattern of serious aggressive behaviors toward self, others or property
 - (c) Constant vocalizations (on average of fifteen (15) minutes of each waking hour), such as screaming, crying, laughing or verbal.

CES services include personal assistance, professional services, home modifications, assistive technology, specialized medical equipment and supplies, and community connection services. Families need to apply through their local Community Centered Board (e.g., DDRC).

DDRC BEHAVIORAL HEALTH SERVICES (not a required service)

The DDRC Board of Directors approved Jefferson County mil levy dollars to fund a Behavioral Health Services team to address unmet behavioral and mental health needs. The Behavioral Health Team provides an internal screening and assessment process to address mental health issues affecting DDRC consumers.

The team includes a Behavior Analyst, Behavioral Health Nurse, and a Psychiatrist. The team reviews referrals and makes appropriate service recommendations. Services may

include consultation, behavior assessment and intervention, care coordination, psychiatric assessment, and medical and medication review. The DDRC Behavioral Health Team collaborates with other community agencies to build capacity and provide a systematic approach in the treatment of children and adults with developmental disabilities and mental health issues. Interested families should contact their DDRC Resource Coordinator.

BEHAVIOR PHARMACOLOGY CLINIC (Offered by DDD)

The Behavior Pharmacology Clinic is a traveling interdisciplinary consultation team provided free of charge to persons with developmental disabilities who are felt to be especially complicated from a behavioral, medical or medication standpoint. The team is designed to support, enhance and educate, not replace local resources. The goal of the clinic is to provide a comprehensive assessment of the individual and to develop a treatment plan that leads to the remission of symptoms, maximizes functioning and enhances the individual's overall quality of life. For more information families should contact their DDRC Resource Coordinator.

2. Services to be contributed to this project and amounts associated with those services:

DDRC will be responsible for:

- Active participation in the IOG as a voting member
- Assignment of a Resource Coordinator to all eligible children. The Resource Coordinator will attend interagency meetings to assist in the identification of needs and make referrals to appropriate services and supports (see above)

3. Staff who will contribute to those services and amounts associated with those staff:

- DDRC currently has 14 Children and Family Services Resource Coordinators serving 1382 children ages birth to 21
- DDRC's Children and Family Services Manager or designee will participate in the IOG meetings.

4. In-kind contributions and the amounts associated to those contributions:

- IOG staff time \$1200
- IOG lunches \$200
- DDRC Children and Family Services staff time (as needed) \$21/hour
- Team Decision-Making staff time \$1200
- Space for meetings, as needed \$400
- Attendance at Options staffings, as needed \$1000

5. Funding sources

The vast majority of funding for services are appropriated from the Colorado Legislature and administered through the Colorado Department of Human Services (CDHS). Within CDHS, DDD is directly responsible for adult services funding and for funding to children

and their families. There is no entitlement to funding or services within the developmental disabilities system; therefore not everyone who is eligible for services receives services. There are waiting lists for services. It is the CCBs responsibility to determine through the Individualized Planning (IP) process what level of support an individual requires and how much funding is necessary to meet the needs of each eligible person based on that person's IP.

Funding for Children and Family Services:

Most of the funding for children and family services is State General Funds, with the exception of the CES program which is funded through Medicaid (50% State general funds and 50% federal Medicaid dollars). 3-5% is local match (e.g. county mill levy funds, cash donations, in-kind donations, grants etc.).

Families with eligible children living at home may request funding for disability related expenses

State FSSP: \$630,000 (Must be determined Most in Need (MIN) relative to other families)

- Fund 400 families @ \$1500 each per year
- Reserve \$30,000 for emergency/discretionary fund

Jeffco CFS Fund: \$500,000 (Jeffco mil levy funds, must live in Jefferson County)

- Fund 300 families at \$1000 each
- Fund 300 families at \$500 each
- Reserve \$50,000 for emergency/discretionary fund

DDRC Behavioral Health Services (\$250,000 in Jeffco mil levy funds supports this service)

Early Intervention Services (for children ages birth to three years of age)

- Approximately \$592,000 to provide early intervention services to about 400 eligible infants and toddlers and their families (e.g.; SLP, OT, PT, and Early Childhood Education) in a four county area.
- Services are provided using a funding hierarchy which includes private insurance, Medicaid, CHP+ and other available resources.

Children's Extensive Support Medicaid Waiver (CES)

- Statewide waiting list
- Those enrolled have access to an average of \$14,036 in services and supports in addition to Medicaid state plan benefits (EPSDT)
- DDRC currently serves 55 children in the CES Waiver

Children's Home and Community Based Services Waiver (C-HCBS)

- Statewide waiting list
- Those enrolled have access to Medicaid State plan benefits (EPSDT) and case management services (CM billed in 15 minute increments, at \$7.87 per 15 minutes)

J. Family Partnerships:

1. Goal(s):

Mission: Intervention and services for individual families will be family driven respecting legal mandates, individualized, and based on family's strengths and abilities. Family members/Family organizations will regularly participate in decision-making bodies relating to intervention and services.

Vision: All families will have the tools and supports needed to participate fully in intervention and treatment services. Family members/Family organizations will be considered as equal partners and thus will be eligible to share in monies received for services rendered.

2. Services to be contributed to this project:

Participate as a voting member of the Jefferson County Interagency Oversight Group (IOG).

Train and mentor families to advocate for themselves and to participate in decision-making bodies for families as a whole.

Train on other applicable subjects, i.e. "How to navigate the Juvenile Justice and the IEP systems."

Continue to build capacity of family organizations in Jefferson County to provide trained family members to serve on committees, boards, ISSTs, etc. and to testify for policy making entities.

Continue to strengthen partnerships and collaboration between the family organizations in Jefferson County.

Be actively involved in the development and implementation of a 1451-specific family outcome survey to assure that family outcomes measured relate to the difference between collaborative and non-collaborative service delivery as well as system of care values and principles.

3. Staff who will contribute to these services and the amounts associated with those staff:

Representatives of the board or staff of JFSN and members of the Jefferson County Affiliate of the Federation of Families will attend and be active members of the IOG meetings at an approximate cost of \$1000.00.

Attend various ISSTs, committees and boards at an approximate cost of \$1440.00.

Train and mentor families at an approximate cost of \$6000.00.

4. Funding Sources:

Various public and private grants and volunteer time at \$15.00 per hour, if this person were to be paid.

IV. Oversight group. The Parties agree that there is hereby created an Interagency Oversight Group, "IOG", whose membership shall be comprised of at least one local representative of Jefferson County Department of Human Services, the First Judicial District, including Probation, Jefferson County Department of Health and Environment, Jefferson County School District, Jefferson Center for Mental Health, Foothills Behavioral Health, Division of Youth Corrections, Developmental Disabilities Resource Center and the Jefferson County Chapter of the Federation of Families for Children's Mental Health, Colorado Chapter in Partnership with the Jefferson County Family Support Network, each such Party having voting member status. Membership requirements are:

1. Attend and actively participate in regularly scheduled meetings;
2. Represent an agency or organization while simultaneously viewing services to families and children on a systems-level;
3. Approve the contribution of time, resources, and/or funding to solve problems;
4. Serve at least a 1 year term of office as an IOG member;
5. Find and nominate an appropriate individual from within their current agency or organization to serve as a replacement if they must discontinue service mid-term.
6. Assume personal responsibility to read reports, make recommendations and manage conflict;
7. Comply with the Memorandum of Understanding Pursuant to House Bill 04-1451 and other documents and agreements pertaining to House Bill 1451;
8. Commit to problem solving and decision making through consensus, realizing that voting is only resorted to when an intractable impasse is reached.

Consensus is defined as all voting members being able to live with and support the decision. When there are multiple representatives of an entity on the IOG, those members need to agree on the one vote for that entity. If they cannot agree, they will abstain. If an IOG representative believes it is inappropriate or a conflict of interest for he or she to vote on a particular decision, that representative shall abstain.

The IOG will strive to resolve all disputes through consensus following a discussion led by the Chair. If consensus is not achieved the members will vote and the majority will prevail. Two-thirds of voting members need to be present in order to vote.

Officers for the first year will be selected by the members of the current standing IOG on or before July 1, 2006. Officers of the IOG shall be elected annually, thereafter, by a majority vote each September beginning in September 2007. Officers shall assume office upon election and serve for one year or until their successors are elected. Officers will include one Chair, one Vice-Chair, one Treasurer and one Secretary. These officers and the other members of the IOG will develop and abide by by-laws for the ongoing operation of the IOG.

In the event that the IOG identifies a need for a subcommittee, the IOG will identify the necessary members for the subcommittee, which may include both members of this MOU as well as other community members. The subcommittee shall report back to the IOG and the subcommittee shall be dissolved upon the completion of the assigned task.

Other voting and non-voting members may be included in the IOG membership by consensus. If consensus can not be reached, the process for resolving disputes will be implemented.

V. Collaborative Management Processes. The collaborative management processes shall address risk-sharing, resource-pooling, performance expectations, outcome-monitoring, and staff training in order to do the following:

- A. Reduce duplication and eliminate fragmentation of services provided to recipients;
- B. Increase the quality, appropriateness, and effectiveness of services delivered to recipients, to achieve better outcomes; and
- C. Encourage cost sharing among service providers.

Jefferson County is developing a Systems of Care (SOC) model to promote the welfare of children through sustainable partnerships that provide integrated, quality services that are individualized, strength based, family centered and culturally competent. This SOC will increase the array of services available to meet the unique needs of children and families through shared resources. Joint treatment planning through ISSTs will reduce duplication and fragmentation of services and encourage sharing of risks and costs among agencies.

Cross-systems training has been implemented and/or supported through Jefferson County's "Improving Child Welfare Outcomes through Systems of Care" federal grant and/or partner agencies to increase knowledge that will enhance collaboration and best practice. The SOC grant has a cross-systems training coordinator. Staff attendance at these cross-system trainings from multiple agencies have and will assist in the quality, appropriateness and effectiveness of services to recipients and will assist in improving outcomes.

SOC has a Parent Partner Coordinator who is working to select, train, and support families who have successfully completed their involvement in the Child Welfare System so that these families can participate effectively in decision making forums and train, mentor and advocate for families currently in the Child Welfare system. The SOC Advisory group and its sub-committees include parent partners who are helping design and implement the SOC, including being involved in the SOC evaluation subcommittee to evaluate the effectiveness of the SOC grant.

The SOC Training Coordinator and Parent Partner Coordinator will be available until September 30, 2008. The goal is to sustain these efforts after the SOC grant ends.

Collaborative management (CM) partners will work together to achieve selected outcomes that are of mutual benefit to our agencies and shared clients, and will pool existing data bases and resources to measure achievement of these outcomes.

CM partners also participate in the CYF Child Protection Team, Options, Team Decision Making Meetings, Systems of Care Advisory Group and sub-committees and Core Services Commission to collaboratively improve and manage services at the individual, system and service delivery level.

VI. Individualized Service and Support Teams. According to the legislation the IOG is authorized to create individualized service and support teams, (hereinafter “ISST”) to develop a service and support plan and provide services to recipients.

The partners to this collaborative will utilize several already existing collaborative forums as ISSTs (see below). The IOG will strengthen the existing groups by expanding partner agency representation. An ongoing assessment of the need for additional ISSTs will be done. These teams will adhere to the underlying principles of a Systems of Care: Interagency and Community Collaboration, Cultural Competence, Family Involvement, Individualized Strength-Based Care Practice and Accountability.

CYF is increasing utilization of Team Decision Making (TDM) which is a component of the Family to Family model. This is a forum that brings together the family, youth, community and partner agencies to develop treatment plans with a trained facilitator. Through this process, families can participate in the development of their treatment plans and share in decisions regarding the care of their children.

CYF is also the lead agency for the Jefferson County “Options” process to bring together agency partners and families to develop alternatives to restrictive levels of out of home care.

Probation has a joint planning process for delinquent youth possibly entering the Department of Youth Corrections.

The IOG will work to improve participation from families and partner agencies in these ISSTs and plan for ways in which they can become more integrated.

VII. Authorization to Contribute Resources and Funding. Each Party to this MOU represents that it has the authority to approve the contribution of time, resources, and funding to solve problems identified by the IOG in order to create a seamless, collaborative system of delivering services to recipients.

VIII. Reinvestment of Moneys Saved, Pooled and Incentive Money Received. The IOG has created a procedure that will be subject to the approval of the head or director of each party agency, to allow any moneys resulting from waivers granted by the federal government and any state general fund savings realized as a result of the implementation of services provided to recipients pursuant to this MOU, to be reinvested by the parties to this agreement in order to provide appropriate services to recipients.

Jefferson County agrees that any savings from the block grant allocation to the county which may result in the State Fiscal Year (SFY) 2007-08 will not be returned to the county. In the event that Jefferson County overspends the allocation for said SFY the county will be allowed to participate in the surplus distribution process should there be such a process.

The percentage of dollars to be spent on delinquency and D & N children and families shall be divided equally unless the IOG decides otherwise.

Jefferson County continues to participate in the State Steering Committee Meetings to expand our knowledge related to collaborative management including how to measure and reinvest possible money saved, pooled funding and incentive money received through this process. IOG members also sit on various committees in their line of work and bring information regarding collaborative management back to the IOG.

Members of the IOG will continue to gain information about evidence-based programs and other successful programs by attending workshops and reading information on such programs and bringing this information back to the group. The IOG will also work with other departments throughout the state to become more knowledgeable about programs that are working in their communities and seek to ascertain if they could be replicated in Jefferson County.

At least yearly, the IOG shall devote an entire meeting to the presentations of programs and services it deems necessary in order to best serve children and families in the community. These programs and services will then be prioritized by the IOG and ranked according to that priority. Funds from any money saved, pooled and/or incentive money will be used to fund such programs and services.

The IOG will create a contract and a budget for each program or service, if necessary, that is chosen to be funded from any money saved, pooled and/or incentive money. The Treasurer will prepare a budget, present it to the IOG for approval and keep track of all monies spent. The Treasurer will get the appropriate signature for expenses being paid and will make quarterly reports to the IOG regarding the financial status of the collaborative.

In the event the IOG disbands, the IOG will meet to discuss how to disburse any unappropriated funds.

The Jefferson County IOG, has final decision making authority on all fiscal matters concerning this MOU and will not recommend any program, policy or this IOG to overspend their budget.

IX. Performance-Based Measures. The Parties hereby determine that they will attempt to meet or exceed the following performance-based measures:

A. Child Welfare Outcome:

Increase the percentage of placement changes where the reason for the change is directly related to helping the child achieve the goals in his/her case plan by 4.1%.

Data source will be State Administrative Review Division's Performance Improvement Plan Report six month rolling average ending June 30, 2008.

Baseline data will be taken from the ARD PIP Report dated March 31, 2007 which shows that Jefferson County is at 66.9%. New outcome will be at least 71%.

B. Juvenile Justice System Outcome:

Decrease the number of revocations of probation by technical violations of youth by 3%.

Data source will be from a Jefferson County Probation Department spreadsheet for the period July 1, 2007 ending June 30, 2008.

Baseline will be taken from a Jefferson County Probation Department spreadsheet for the time period April 1, 2006-March 31, 2007.

C. Education Outcome:

Increase attendance rates of CYF children attending public schools for at least 60 consecutive school days and are over the age of four, in kindergarten or higher by 1%.

Data source will be from Trails cross-referenced with Infinite Campus for the 2007-2008 school year.

Baseline will be taken from Trails cross-referenced with Infinite Campus for the 2006-2007 school year.

D. Health/Mental Health/Other Outcome:

For the time frame of July 1, 2007 - June 30, 2008, 33% of CYF clients enrolled in the Party Wise Program at the Jefferson County Department of Health and Environment (JCDHE) will increase their readiness to use effective birth control and 33% will increase their readiness to stop at-risk level drinking. Increased readiness for these behaviors will be demonstrated through comparison of pre-test to post-test scores indicated on the FAS-PACE Data Collection Form . The objective of this program is to reduce alcohol-exposed pregnancies in Jefferson County by focusing on increasing contraception and/or decreasing drinking.

Data source will come from an Excel Spreadsheet created by JCDHE and sent to the Colorado Department of Public Health and Environment (CDPHE) who puts it into an Access Database for the Fetal Alcohol Syndrome Prevention Program.

Baseline will come from an Excel Spreadsheet that is sent to CDPHE who then puts the information into an Access Database for the Fetal Alcohol Syndrome Prevention Program. The time period will be April 1, 2004, through March 31, 2007, which shows that 65% of the general population in Jefferson County increased their readiness to use effective birth control and 70% increased their readiness to stop at-risk level drinking. We are recommending a lower percentage of clients due to CYF clients being a higher risk population than the general population.

Actual surveys will be kept at the Jefferson County Department of Health and Environment.

The IOG will submit baseline data for Juvenile Justice and Education to the State Department of Human Services by September 1, 2007. The percents increased and decreased are the minimum number that will be effected. Data gathering has proven to be more difficult and time consuming than anticipated so it is difficult to predict the percent change at the time of this writing.

X. Confidentiality Compliance. Parties agree that State and Federal law concerning confidentiality shall be followed by the Parties and IOG. Any records used or developed by the IOG or its members or by the ISST that relate to a particular person are to be kept confidential and may not be released to any other person or agency, except as provided by law.

A release of information that covers the confidentiality needs of all Parties and will then only need to be signed by Recipients one time to better facilitate the exchange of information is being discussed.

XI. Termination of MOU. The Parties acknowledge that withdrawal from this MOU of any statutorily required Party will result in the automatic termination of this Agreement and termination of the collaborative system of delivery of services developed hereunder. The withdrawing Party shall assist the other Parties to achieve an orderly dissolution of the collaborative system with as little disruption as possible in the delivery of services provided to Recipients.

A. Withdrawal/Termination Any Party may withdraw from this Agreement at any time by providing 30 days written notice to all other Parties.

B. For Loss of Funds. Any Party may withdraw from this Agreement, or modify the level of its commitment of services and resources hereunder, effective immediately, in the event of loss or reduction of resources from its funding source identified herein. Any Party withdrawing due to loss of funds will provide notice of withdrawal, in writing within 30 days.

IN WITNESS WHEREOF, the Parties hereto, through their authorized representatives have executed this Memorandum of Understanding effective for the dates written above.

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE JEFFERSON COUNTY DEPARTMENT OF HUMAN SERVICES

By: _____ Date _____

Its: _____

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE FIRST JUDICIAL DISTRICT

By: _____ Date _____

Its: _____

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE JEFFERSON COUNTY PROBATION DEPARTMENT

By _____ Date _____

Its: _____

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE JEFFERSON COUNTY DEPARTMENT OF HEALTH AND ENVIRONMENT

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of _____ be effective as of _____.

JEFFERSON COUNTY DEPARTMENT
OF HEALTH AND ENVIRONMENT

CONTRACTOR

Cathy Corcoran, President
Board of Health

SSN /EIN

ATTEST: _____

By: Bonnie McNulty, Secretary
Board of Health

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE JEFFERSON COUNTY SCHOOL DISTRICT

By: _____ Date _____

Its: _____

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE JEFFERSON CENTER FOR MENTAL HEALTH

By: _____ Date _____

Its: _____

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

FOOTHILLS BEHAVIORAL HEALTH

By: _____ Date _____

Its: _____

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE JEFFERSON COUNTY DEVELOPMENTAL DISABILITIES RESOURCE
CENTER

By: _____ Date _____

Its: _____

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE DIVISION OF YOUTH CORRECTIONS

By: _____ Date _____

Its: _____

FOR JEFFERSON COUNTY
MEMORANDUM OF UNDERSTANDING
PURSUANT TO HOUSE BILL 04-1451

THE JEFFERSON COUNTY CHAPTER OF THE FEDERATION OF FAMILIES FOR
CHILDREN'S MENTAL HEALTH, COLORADO CHAPTER IN PARTNERSHIP
WITH THE JEFFERSON COUNTY FAMILY SUPPORT NETWORK

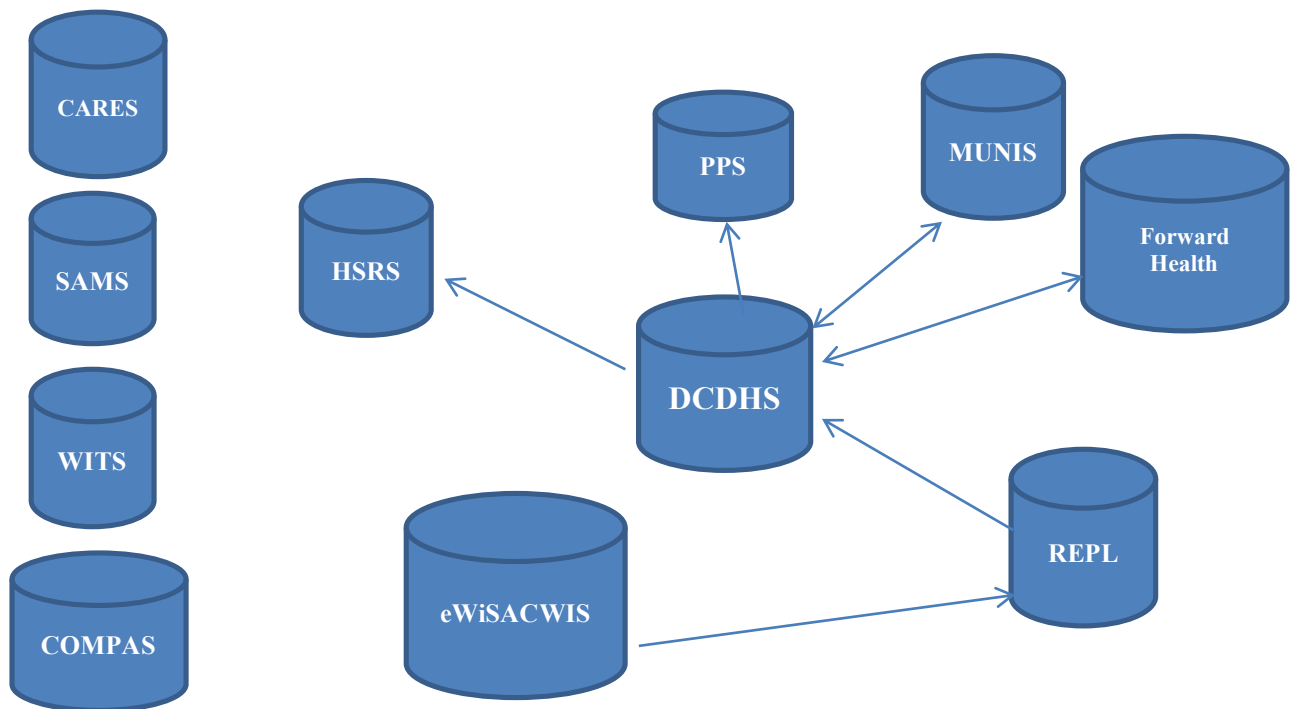
By: _____ Date: _____

Its: _____

Appendix D: DCDHS Database Communication Structure

Note: This information was provided to the authors by DCDHS staff in the form of a working document. It is not complete and is only intended to provide a brief overview of the various systems and applications used by the organization.

External Applications



Client Assistance for Re-Employment and Economic Support System (CARES/ACCESS)

CARES/ACCESS are the application, eligibility and account management systems for the State of Wisconsin's Income Maintenance Programs – Medicaid, BadgerCare Plus, FoodShare, and Caretaker Supplemental. Data is keyed by DCDHS staff directly into CARES. ACCESS allows clients to apply for benefits and to access their accounts.

Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)

This is a web-based application by Northpointe, Inc. designed to assess the risk of recidivism among offenders. The program has been used by the Wisconsin Department of Corrections since 2012. DCDHS staff key directly into COMPAS.

ForwardHealth Portal

The ForwardHealth Portal, under the auspices of the Wisconsin Department of Health Services, is the interface to the ForwardHealth Interchange, the Medicaid Management Information System for the State. Through this, claims for eligible members may be

submitted for reimbursement. To obtain reimbursement under the Comprehensive Community Services (CCS) program, DCDHS, following the 837 specifications, uploads data files on a monthly basis and retrieves an 835 file with information regarding claim status and reimbursement.

Human Services Reporting System (HSRS) – Long Term Support Module

Housed in the Wisconsin Department of Health Services, the Human Services Reporting System (HSRS) is a web-based reporting tool used to collect data on several social service and disability service programs operated by counties and funded by federal, state, and local funds. County agencies use this system to report to the state on the individual clients they are serving, the services they provide, and their expenditures. Much of their state and federal funding is either directly or indirectly determined by what they report in this system. This is used to report services under the Children's Long-Term Support Waiver (CLTS-W). Dane County utilizes a batch file transfer to submit data from the DCDHS Information System to HSRS.

Municipal Uniform Information System (Munis)

In 2004, Dane County selected Tyler Technologies, Inc.'s financial, human resource, and revenue software known as Munis. This serves as the County's general ledger system.

Program Participation System (PPS)

Housed in the Wisconsin Department of Health Services, PPS is a web-based electronic client-level data collection system for reporting to the State of County-authorized or paid for substance abuse and/or mental health services. The data collected for the AODA and Mental Health Modules meets both State and federal reporting requirements. It includes basic client demographics, services, and outcomes associated with those services. Dane County utilizes a batch file transfer to submit data from the DCDHS Information System to PPS.

Social Assistance Management System (SAMS)

SAMS is used by the Aging and Disability Resource Center (ADRC) for its Call Center and by the Area Agency on Aging (AAA) for its nutrition program. For the ADRC, the system collects caller information, notes, and profiles and is able to generate several standardized reports on Call Center activities and the outcomes of those calls. DCDHS staff key data directly into this system.

Wisconsin Incident Tracking System (WITS)

This is a web-based system that collects information for the Wisconsin Department of Health Services (DHS). This system collects information on each county's response to incidents of suspected abuse, financial exploitation, neglect, and self-neglect among elders and adults at risk. The system generates aggregate reports for each County and annual reports for the State as a whole. DCDHS Adult Protective Services (APS) staff key directly into this system.

Wisconsin Statewide Automated Child Welfare Information System (eWiSACWIS)

Implemented in Dane County February 23, 2004, SACWIS is a web-based comprehensive, automated case management tool that supports child welfare practice throughout the State of Wisconsin. Maintained in the Department of Family It is intended to hold the State's official case record, which includes a complete, current, accurate, and unified case management history on all children and families served by the State's or Tribe's title IV-B and title IV-E entities. SACWIS also supports the reporting of the data for both the Adoption and Foster Care Analysis Review System (AFCARS) and the National Child Abuse and Neglect Data System (NCANDS), a voluntary national data collection and analysis system. DCDHS staff key enter data directly into this system. There is a REPL database that the State populates for use by counties. Dane County bring back this data for cutting checks to facilities, such as foster homes and group homes for children placed out of home. Placement data is also brought into the Mental Health Module of the DCDHS Information System.

Internal Applications

DCDHS uses multiple internal applications, including applications that were developed in-house and applications that were purchased and customized. Internal applications include Access database applications and Excel spreadsheets that are used for tracking program and financial data. DCDHS operations also utilize over 1,000 Access databases throughout the Department, however many of these are single-user applications.

Appendix E: Recommended Readings

This list is intended to highlight a few key resources and readings. Over the course of this project, we read over 50 governmental reports, scientific papers, various presentations and IDS websites. The following ten resources are ones we found to be extremely helpful and are must reads.

1. Actionable Intelligence for Social Policy

- This website is a comprehensive, user-friendly guide to the creation of an IDS. In addition to the many resources and sample documents provided on the website, they coordinate an IDS network for governments developing an IDS.
- <https://www.aisp.upenn.edu/>

2. “The Integrated Data System Approach: A Vehicle to More Effective and Efficient Data-Driven Solutions in Government”

- This report is similar to ours, offering a comprehensive look at what an IDS is and how to create one.
- https://www.aisp.upenn.edu/wp-content/uploads/2017/09/The-IDS-Approach_Fantuzzo-et-al.-2017_Final.pdf

3. “Sharing Data for Better Results” toolkit by the National League of Cities

- This is a toolkit which provides information on how to balance privacy rights, deliver effective services, keep the public informed, ensure compliance with laws and regulations and operate more efficiently
- <http://www.nlc.org/sharing-data-for-better-results>

4. “Connecting the Dots: The Promise of Integrated Data Systems for Policy Analysis and Systems Reform”

- The legal, ethical, scientific and economic challenges of interagency data sharing are examined. A survey of eight integrated data systems, including states, local governments and university-based efforts, explores how the developers have addressed these challenges. Some exemplary uses of the systems are provided to illustrate the range, usefulness and import of these systems for policy and program reform. Recommendations are offered for the broader adoption of these systems and for their expanded use by various stakeholders.
- https://repository.upenn.edu/spp_papers/146/

5. United States Governmental Accountability Office: “Sustained and Coordinated Efforts Could Facilitate Data-Sharing While Protecting Privacy”

- This report looked at four locations - Michigan, Utah, Alleghany County and New York City- and systematically detailed their IDS implementation challenges,

structure, and benefits. They also discussed how the federal government is and can better support these systems in the future.

- <https://www.gao.gov/products/GAO-13-106>

6. Human Services Integration Fund (HSIF)

- This document explains the HSIF used in Alleghany County to fund their IDS project
- <http://www.county.allegheny.pa.us/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=2147486026>

7. Legal Issues for IDS Use: Finding a Way Forward

- This resource details common privacy concerns, MOUS and DULs and specific laws.
- <https://www.aisp.upenn.edu/wp-content/uploads/2016/07/Legal-Issues.pdf>.

8. “Critical Attributes of Organizational Culture that Promote Knowledge Management Technology Implementation Success” by Heejun Park, Vincent Ribiere and William Schulte Jr.

- This article examines the characteristics of organizations that lead to successful IDS implementation.

9. Super-Utilizer Summit: Common Themes from Innovative Complex Care Management Programs

- The Center for Health Care Strategies (CHCS), in partnership with the National Governors Association, hosted a *Super-Utilizer Summit* on February 11 and 12, 2013 which brought together leaders from super-utilizer programs across the country. This report presents the *Summit’s* common themes and key recommendations for building better systems of care for high utilizers.
- https://www.chcs.org/media/FINAL_Super-Utilizer_Report.pdf.

10. Pardo and Tayi Framework: “Interorganizational information integration: A key enabler for digital government”

- This paper explains a framework for approaching IDS. See appendix A for more details.

References

1. Program Overview – UniverCity Alliance – UW–Madison. <https://university.wisc.edu/ucy/>. Accessed November 19, 2017.
2. Gawande A. The Hot Spotters. *The New Yorker*. http://www.cbhc.org/news/wp-content/uploads/2011/02/Lower-Costs-and-Better-Care-for-Neediest-Patients_-_The-New-Yorker.pdf. Published January 24, 2011.
3. FUSE Initiative. Corporation for Supportive Housing. <http://www.csh.org/csh-solutions/community-work/introduction-to-systems-change/fuse/fuse-overview/>.
4. Hasselman D. *Super-Utilizer Summit: Common Themes from Innovative Complex Care Management Programs*. Center for Health Care Strategies; 2013. https://www.chcs.org/media/FINAL_Super-Utilizer_Report.pdf.
5. Johnson TL, Rinehart DJ, Durfee J, et al. For Many Patients Who Use Large Amounts Of Health Care Services, The Need Is Intense Yet Temporary. *Health Aff (Millwood)*. 2015;34(8):1312-1319K. doi:10.1377/hlthaff.2014.1186.
6. W. Warning, Wood J, Letcher A, Srouji N, Echterling C, Carpenter C. *Working With the Super-Utilizer Population: The Experience and Recommendations of Five Pennsylvania Programs*. AF4Q; 2014. doi:http://inside.fammed.wisc.edu/applications/chpp/documents/publications/PopulationHealth/Pennsylvania%20Programs_High_Utilizer_report.pdf.
7. Project 25: Dramatic Cost Savings of Public Resources. <https://uwsd.org/Project-25-Dramatic-Cost-Savings-of-Public-Resources>. Published November 16, 2011. Accessed November 14, 2017.
8. Stanton M. *The High Concentration of U.S. Health Care Expenditures*. Rockville (MD): Agency for Healthcare Research and Quality; 2005. https://meps.ahrq.gov/data_files/publications/ra19/ra19.pdf.
9. Culhane DP, Fantuzzo J, Rouse HL, Tam V, Lukens J. *Connecting the Dots: The Promise of Integrated Data Systems for Policy Analysis and Systems Reform*. Intelligence for Social Policy - University of Pennsylvania; 2010.
10. Ramon Gil-Garcia J, Chengalur-Smith I, Duchessi P. Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector. *Eur J Inf Syst*. 2007;16(2):121-133. doi:10.1057/palgrave.ejis.3000673.
11. Pardo TA, Tayi GK. Interorganizational information integration: A key enabler for digital government. *Gov Inf Q*. 2007;24(4):691-715. doi:10.1016/j.giq.2007.08.004.
12. Green-Edwards C. Medicaid and PHA - Partnership in using the Data Warehouse. <http://slideplayer.com/slide/5721815/>. Accessed November 14, 2017.

13. *Human Services - Sustained and Coordinated Efforts Could Facilitate Data-Sharing While Protecting Privacy*. Washington, D.C.: United States Government Accountability Office; 2013.
14. Pittaway L, Robertson M, Munir K, Denyer D, Neely A. Networking and innovation: a systematic review of the evidence. *Int J Manag Rev*. 2004;5-6(3-4):137-168. doi:10.1111/j.1460-8545.2004.00101.x.
15. Kotlarsky J, Oshri I. Social ties, knowledge sharing and successful collaboration in globally distributed system development projects. *Eur J Inf Syst*. 2005;14(1):37-48. doi:10.1057/palgrave.ejis.3000520.
16. Jørgensen TB, Bozeman B. Public Values: An Inventory. *Adm Soc*. 2007;39(3):354-381. doi:10.1177/0095399707300703.
17. Carpenter DP, Krause GA. Reputation and Public Administration. *Public Adm Rev*. 2012;72(1):26-32. doi:10.1111/j.1540-6210.2011.02506.x.
18. Kitzmiller E. *Allegheny County's Data Warehouse: Leveraging Data to Enhance Human Service Programs and Policies*. Philadelphia, PA: University of Pennsylvania; 2014.
19. van Panhuis WG, Paul P, Emerson C, et al. A systematic review of barriers to data sharing in public health. *BMC Public Health*. 2014;14(1):1144. doi:10.1186/1471-2458-14-1144.
20. Freedman Consulting LLC. A Guide to Facilitating Technology Innovation in Human Services.
21. Human Services Integration Fund (HSIF).
22. *Using the Enterprise Data Warehouse to Improve Delivery of Health Care Services*. State of Michigan Department of Community Health
<https://www.nga.org/files/live/sites/NGA/files/pdf/ITTOOLKITBPMI.pdf>. Accessed November 14, 2017.
23. *Achieving Breakthrough Results in Health Care Delivery, Management, and Cost Containment*. Department of Community Health, Department of Information Technology
<https://www.nascio.org/portals/0/awards/nominations2007/2007/2007MI3-MI%20NASCIO%20-%20DCH%20Data%20Warehouse%20Nomination%20-%206.6.07.pdf>. Accessed November 14, 2017.
24. Gill S, Dutta-Gupta I, Roach B. Allegheny County, Pennsylvania: Department of Human Services' Data Warehouse. Data-Smart City Solutions.
<http://datasmart.ash.harvard.edu/news/article/allegheny-county-pennsylvania-department-of-human-services-data-warehouse-4>. Published June 11, 2014. Accessed November 14, 2017.

25. DHS Data Warehouse. DHS Data Warehouse. <http://www.alleghenycounty.us/Human-Services/News-Events/Accomplishments/DHS-Data-Warehouse.aspx>. Accessed November 14, 2017.
26. Dalton E, Gorr W, Lucas J, Pierce J. *Data Warehousing, Flow Models, and Public Policy*. Pittsburgh, PA: Allegheny County Department of Human Services; 2006.
27. Sobkowski I. HHS-Connect: Big Apple, Big Changes. *Doc Stewards Change Learn Cent Httpwww Steward ComLearningCenterDocumentsTHOUGHTLEADERSHHS 20Connect 20Big 20Apple Pdf*. 2009.
28. Watson HJ, Goodhue DL, Wixom BH. The benefits of data warehousing: why some organizations realize exceptional payoffs. *Inf Manage*. 2002;39(6):491-502. doi:10.1016/S0378-7206(01)00120-3.
29. Sobkowski I, Freedman RS. The Evolution of Worker Connect: A Case Study of a System of Systems. *J Technol Hum Serv*. 2013;31(2):129-155. doi:10.1080/15228835.2013.772010.
30. Patterson D, Brennan N, Haeberlen A, Schroeder A, Smith A, Steif K. *Towards State-of-the-Art IDS Technology and Data Security Solutions*. Philadelphia, PA: Actionable Intelligence for Social Policy, Expert Panel Report; 2017. <https://www.aisp.upenn.edu/wp-content/uploads/2016/07/Technology-Data-Security.pdf>. Accessed November 14, 2017.
31. Schein EH. *Organizational Culture and Leadership*. 3rd ed. San Francisco: Jossey-Bass; 2004.
32. Park H, Ribière V, Schulte WD. Critical attributes of organizational culture that promote knowledge management technology implementation success. *J Knowl Manag*. 2004;8(3):106-117. doi:10.1108/13673270410541079.
33. Kitzmiller E. *Washington State's Integrated Client Data Base and Analytic Capacity*. Philadelphia, PA: University of Pennsylvania; 2014.
34. Peled A. When transparency and collaboration collide: The USA Open Data program. *J Am Soc Inf Sci Technol*. 2011;62(11):2085-2094. doi:10.1002/asi.21622.
35. Kingdon JW. *Agendas, Alternatives, and Public Policies*. Harlow: Pearson Education Limited; 2014.
36. Kerwin CM, Furlong SR. *Rulemaking: How Government Agencies Write Law and Make Policy*. Washington, D.C: CQ Press; 2011.
37. *AN ACT TO PROMOTE EFFICIENCY AND EFFECTIVENESS IN THE ADMINISTRATION OF HUMAN SERVICES AND TO STRENGTHEN THE LOCAL PUBLIC HEALTH INFRASTRUCTURE BY ESTABLISHING A PUBLIC HEALTH IMPROVEMENT INCENTIVE PROGRAM AND ENSURING THE PROVISION OF THE*

TEN ESSENTIAL PUBLIC HEALTH SERVICES. Vol North Carolina Session Law 2012-126.

38. Wall AN, Moore JD, Berner M, Foster J, Markiewicz M. *Comparing North Carolina's Local Public Health Agencies: The Legal Landscape, the Perspectives, and the Numbers*. Chapel Hill, NC: University of North Carolina; 2013.
39. Fairchild AL, Gable L, Gostin LO, Bayer R, Sweeney P, Janssen RS. Public goods, private data: HIV and the history, ethics, and uses of identifiable public health information. *Public Health Rep*. 2007;122(1_suppl):7–15.
40. Rosenbaum S. Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access. *Health Serv Res*. 2010;45(5 Pt 2):1442-1455. doi:10.1111/j.1475-6773.2010.01140.x.
41. Gostin LO, Hodge JG, Valdiserri RO. Informational Privacy and the Public's Health: The Model State Public Health Privacy Act. *Am J Public Health*. 2001;91(9):1388-1392.



About UniverCity Year

UniverCity Year is a three-year partnership between UW-Madison and one community in Wisconsin. The community partner identifies sustainability and livability projects that would benefit from UW-Madison expertise. Faculty from across the university incorporate these projects into their courses with graduate students and upper-level undergraduate students. UniverCity Year staff provide administrative support to faculty, students and the partner community to ensure the collaboration's success. The result is on-the-ground impact and momentum for a community working toward a more sustainable and livable future.

UniverCity Alliance

univercityalliance@wisc.edu

608-890-0330

univercity.wisc.edu



UniverCity Alliance
UNIVERSITY OF WISCONSIN-MADISON