2018-2019

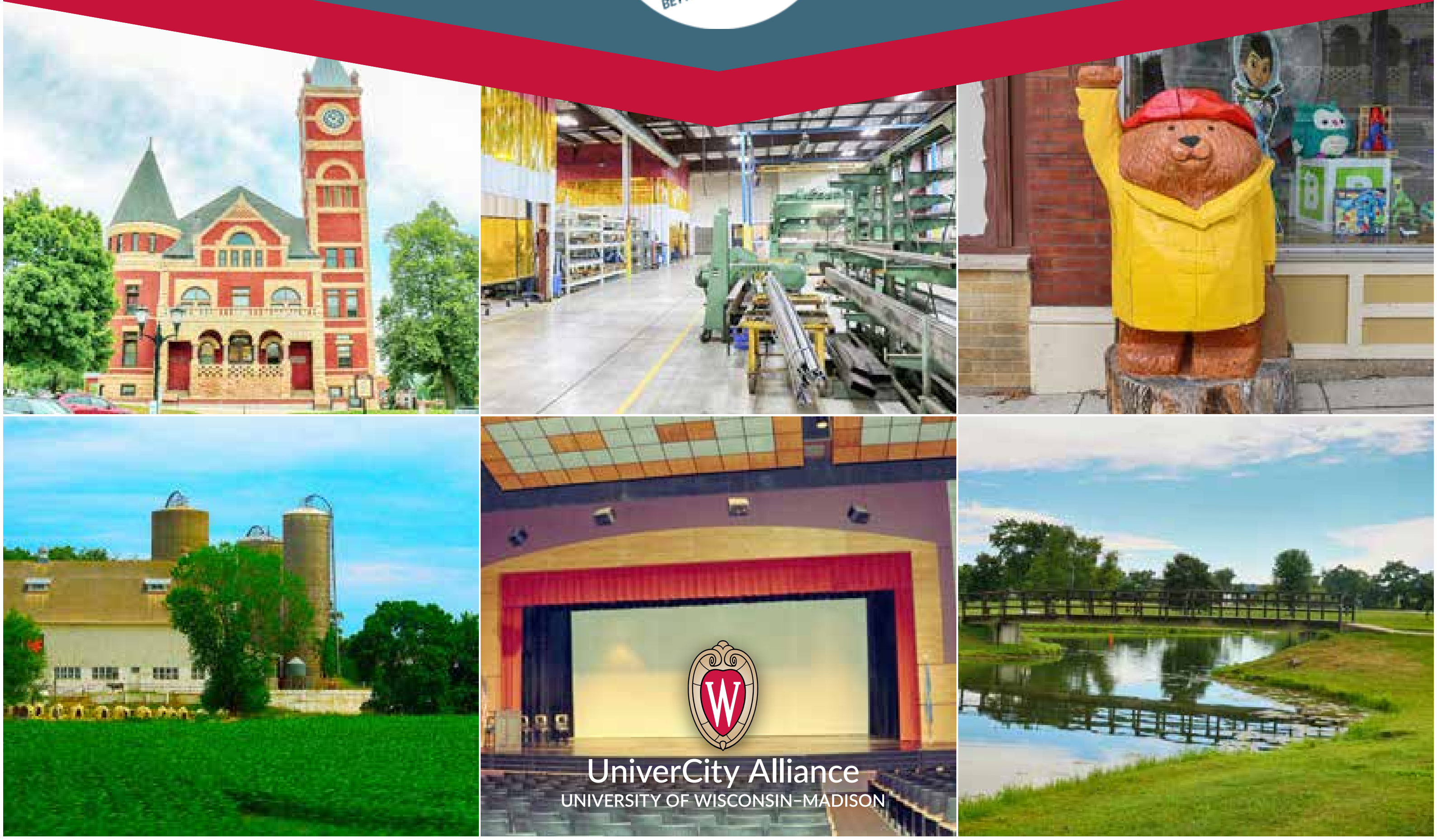
FINAL REPORT

UniverCity Year

Better • Places • Together

Data sharing to combat the opioid crisis in Green County

POPULATION HEALTH SCIENCES 780: PUBLIC HEALTH: PRINCIPLES AND PRACTICE



UniverCity Alliance

UNIVERSITY OF WISCONSIN–MADISON

Table of Contents

Acknowledgements iii
UniverCity Year - University of Wisconsin iv
Opioid Crisis in Green County 1
The Need for Data Sharing 1
Types of Data Sharing Systems 2
Maps 2
Data Dashboards 2
Integrated Data Systems (IDS) 3
Health Information Exchanges (HIE) 3
Opioid-Related Metrics 3
Healthcare-Related Opioid Metrics 3
Opioid Overdoses - Fatal 3
Opioid Overdoses - Non-Fatal 4
Opioid Use Disorder, Medication Assisted Treatment, and Chronic Non-Malignant Pain 4
Opioid Prescribing Practices 5
Narcan/Naloxone Use 5
Law Enforcement 6
Opioid-Related Arrests 6
District Attorney 6
Court System 7
Drug Courts 7
Benefits of Data Sharing Systems 7
Improved outcomes 7
Increased efficiency and cost savings 8
Increased organizational capacity 8
Improved grant funding 8
Increased interorganizational collaboration 8
Improved accountability 9
Barriers 9
Funding 9
Initial funding areas 10
Data Management 10
Sharing Data 10
Data Analysis 11
Maintenance Funding 12
Technical Barriers 12

System Structure 13
Security 14
Organizational Culture as a Barrier to IDS Implementation 15
Political and Cultural Barriers 16
Legal Barriers 16
Health Insurance Portability and Accountability Act of 1996 (HIPAA) 17
42 CFR Part 2 17
Other Legislative and Regulatory Considerations 18
Key Considerations in Creating Data Sharing System 18
Data Sharing Agreements and Memoranda of Understanding 18
Recommendations 20
Short Term (High Priority) 20
Mid Term (Medium Priority) 21
Long Term (Low Priority) 23
Conclusion 25
References 26
Appendix A: Examples of Data Sharing Initiatives 30
Appendix B: Examples of Data Sharing Agreements 36
Appendix C: Logic Model 71

Acknowledgements

We would like to thank the Green County Criminal Justice Coordinating Council (CJCC) for creating this opportunity to support this important opioid initiative. We greatly appreciate the CJCC members who took the time to speak with us - in particular, Bob Gibson, Sheriff Mark Rohloff, Wes Speer, and Brian Bucholtz - and offer their expertise and guidance.

Additionally, without the cooperation and support of the Green County Economic Development Corporation and the UniverCity Year project staff, we would never have had the opportunity to work on this project.

We are grateful to the persons who discussed their own data sharing projects with us, including Dr. Mallory O'Brien, Jennifer Hernandez-Meier, Sara Kohlbeck, and Kerianne Guth, as well as Sheri Johnson for connecting us with many of these individuals.

Finally, we would like to thank Samantha Aisen and Professor Barbara Duerst for their guidance and support throughout this project.

UniverCity Year - University of Wisconsin

This project was completed in partnership with UW-Madison’s UniverCity Year, a program that helps local government leaders throughout Wisconsin find practical solutions to their toughest challenges. We are grateful for the support of the community members and the UniverCity Year staff.

Opioid Crisis in Green County

The Healthy Community Coalition of Green County, WI, has identified reducing substance abuse as a high priority goal (Green County, 2018). Opioid use in particular is concerning; Wisconsin as a whole is in the midst of a drug overdose epidemic driven by opioids (Wisconsin DHS, 2017). Between 2013-2015, Green County had 7 overdose deaths involving opioids with a rate of 6.3 opioid overdose deaths per 100,000 persons.

There has been a ten-fold rise in Green Country hospital encounters involving opioids since 2006 (Wisconsin DHS, 2017). Compared to other Wisconsin counties in 2014, Green County is in the highest quintile for rates of hospitalizations involving opioids in general (58.7 hospitalizations per 100,000 persons), opioid prescriptions (40.6 hospitalizations per 100,000 persons), and heroin poisonings (13.5 hospitalizations per 100,000 persons). Between 2011 and 2015, ambulance runs in Green County where Naloxone was administered has more than doubled, and rates of neonatal abstinence syndrome has steeply increased. Additionally, the number of Green County residents seeking opioid treatment by the Department of Human Services has tripled in recent years (Gibson, 2018).

The Need for Data Sharing

There are multiple stakeholders involved in the opioid epidemic, including law enforcement, courts, jails, healthcare, and emergency medical services (EMS). Each of these stakeholders' perspective is crucial to understanding the broad factors contributing to and driving this opioid use. In Green County, community partners are motivated to address this opioid use, but each stakeholder only has access to part of the data. Community partners must be able to effectively communicate these views, as well as data related to opioids, to develop appropriate solutions.

Currently, Green County stakeholders rely on data from the Department of Health Services for opioid-related health outcomes. This data is often outdated by several years, which leads to delays in fully understanding this rapidly evolving epidemic and makes it difficult to achieve adequate funding and implement programs.

To combat this issue, Green County hopes to develop a platform that will allow for opioid-related data to be shared between agencies. Community partners would update the platform regularly so the data remains relevant and easily accessible. Access to a diverse set of data would improve understanding of local opioid use, help develop policy recommendations to address opioid use, and be a key component of grant application processes, which in turn will provide opportunities to increase funding for opioid related programs in Green County. It is hoped that this data sharing initiative would also increase collaboration between stakeholders and facilitate development of mutual strategies and goals. Overall, this would facilitate a better informed and more efficient approach to the opioid crisis in Green County.

The goal of our project was to create a plan and timeline for the development of a data sharing platform in Green County by analyzing examples and best practices of data sharing initiatives. Below, we have provided community stakeholders with detailed information on appropriate methods for data collection and management, as well as opioid-related metrics to consider including. Our timeline will consist of short, medium, and long-term goals for the community to work towards in addressing the issue of data sharing for opioid use.

Types of Data Sharing Systems

Sharing data is a complex process, but utilizing technology has been shown to improve understanding, efficiency, and effectiveness of the data (Hofman, 2014). There are many systems for sharing data between organizations, each with unique advantages and limitations. Some of the existing systems for sharing information include maps, dashboards, integrated data systems (IDS), and health information exchanges (HIE). The following section discusses a few of the available options for developing a data sharing system along with the associated challenges of each. While the following categories are fixed, there is often overlap between these categories when systems are created. Specific examples from the following systems will be discussed later in this report.

Maps

Maps are data sharing tools that allow you to communicate data spatially based on location and geography. Maps provide a unique way to visualize relationships by layering different information. However, maps are limited to presenting data spatially and may require the data to be in a specific format. Some examples of specific programs to create maps include ArcGIS and ODMAP.

Data Dashboards

A similar method of data sharing is with a data dashboard, which is an information management tool that provides a central location to monitor and analyze the data. Dashboards allow for all metrics to be consolidated and stored in one place, but they may not be the most user-friendly and may require technical assistance from the software developer or an IT professional (Hofman, 2014). An example of a software that allows you to create data dashboards is Tableau. Programming software like *RStudio* could also create tables and figures for a dashboard, but requires experience with the *R* programming language.

Integrated Data Systems (IDS)

IDS link individual level data between multiple agencies (Data Integrated Systems, 2018). IDS can be used to evaluate programs and policies, but may require extensive technical resources and there may be a delay between information in the IDS, in reports, and in reality (Data Integrated Systems, 2018). Examples of IDS include data warehouses, which standardize and store information centrally, or portals, which store the information in separate systems.

Health Information Exchanges (HIE)

HIE are slightly different from the previous three systems in that they only facilitate the sharing of healthcare information. HIE allow the sharing of patient electronic medical records (EMR) within a region, community, or hospital system (Health Information Exchange, 2018). They are limited by the information contained in the medical record. Epic Care Everywhere is an example of an internal HIE.

Opioid-Related Metrics

There are many opioid-related metrics that Green County stakeholders could consider sharing. These span several different domains, including healthcare, law enforcement, the district attorney, and court system.

With more data and metrics shared between stakeholders hopefully comes a better understanding of opioid-related needs in Green County. Additionally, a larger variety of agencies sharing data will create a stronger network of stakeholders and improved buy-in when collaborating to develop and implement comprehensive solutions to the opioid crisis. However, there is a clear trade off -- when including more metrics from a larger number of stakeholders, the data sharing will become more complicated and expensive.

Below, several opioid-related metrics to consider including in this data-sharing project have been outlined. The likely sources of this data have also been included.

Healthcare-Related Opioid Metrics

Opioid Overdoses - Fatal

Fatal overdoses due to opioids are a very important metric to track in Green County. As the opioid epidemic has grown nationally, deaths due to opioid overdoses have also risen dramatically (Kolodny et al, 2015). Having data concerning fatal overdoses, especially in real time, could give Green County stakeholders a better chance at mounting prompt public health responses to overdoses and preventing future deaths. Overdose death locations could also help guide interventions.

In addition to the number of fatal overdoses involving opioids, it may be important to track whether these overdoses were caused by specific drugs, including: prescriptions (e.g. oxycodone, hydrocodone, methadone); heroin; or synthetic (fentanyl or other illicitly manufactured drugs) (Washtenaw County Health Department, 2018). Socioeconomic status for individuals with fatal overdoses could be tracked, which could be further broken down by drug type (Washtenaw County Health Department, 2018). Subcategories of fatal overdoses could include unintentional deaths, intentional deaths, undetermined deaths, and homicide.

Potential data sources include the county coroner/medical examiners; police; emergency medical services; the State Unintentional Drug Overdose Reporting System (SUDORS); or ODMAP (see Appendix A).

Opioid Overdoses - Non-Fatal

Non-fatal opioid overdoses are another important health metric to track over time. Overdoses are one of the clearest manifestations of the opioid crisis, especially as the number of individuals using heroin and fentanyl grow. Non-fatal overdoses also represent an opportunity to intervene, as these individuals are at high risk for future non-fatal and fatal overdoses (Coffin et al, 2007).

Within this category of non-fatal overdoses, there are several related metrics that could be collected, including: hospitalizations due to non-fatal overdoses; ED visits due to non-fatal overdoses; drug causing the overdose, when data is available; and socioeconomic status for individuals with overdoses, which could be further broken down by drug type. Subcategories of these non-fatal overdoses include whether the overdose was intentional, unintentional, undetermined, or an adverse effect of opioid agonist therapeutic medication.

Possible data sources for overdoses include: medical systems in Green County, including the Monroe Clinic; the State Unintentional Drug Overdose Reporting System (SUDORS); emergency medical services; police departments; fire departments; and ODMAP (see Appendix A).

Opioid Use Disorder, Medication Assisted Treatment, and Chronic Non-Malignant Pain

To understand the scope of the opioid epidemic and drug use more broadly, it is important to track the number of persons with documented drug use. The number of patients with a diagnosis of conditions such as Opioid Use Disorder can inform stakeholders of the scope of opioid use in

Green County. Though this is unlikely to capture all drug users, as many people avoid disclosing drug use to healthcare providers, it is still valuable to track over time.

The percent of individuals with Opioid Use Disorder who receive medication assisted treatment and/or psychosocial treatment is valuable information as well. This metric would offer insight about difficulties for patients to accessing adequate treatment, and if providers are appropriately referring patients to treatment options. Tracking other diagnoses in which individuals are commonly (though sometimes inappropriately) prescribed opioids, such as chronic non-malignant pain, could also be useful (Martell et al, 2007).

Specific metrics include the number of individuals diagnosed with these conditions; number of individuals receiving medication-assisted treatment; incidence and diagnosis rate of chronic non-malignant pain, as well as opioid prescriptions for this condition (Minnesota DHS, 2018).

Possible data sources include Alcohol and Other Drug Use of Green County Human Services; Green County medical systems, such as the Monroe Clinic; and data from large surveys such as the National Survey on Drug Use and Health or Behavioral Risk Factor Surveillance Survey (BRFSS).

Opioid Prescribing Practices

Inappropriate opioid prescribing is a significant driver of the opioid crisis. Most individuals who use strong opioids like heroin and fentanyl began with using opioid prescriptions, and inappropriate prescribing is associated with higher mortality and overdoses (Rose et al, 2018). This metric is important because it measures a common local source of opioids for Green County, is amenable to be decreased, and can alert stakeholders about providers that may prescribe more opioids than recommended.

Specific metrics could include: the total number and rates of opioid prescriptions filled, in particular for high dose opioids (>90 morphine milligram equivalents dispensed/day); days of supply per prescription (e.g. less than or greater than a month supply); morphine milligram equivalents dispensed; source of opioid prescriptions (e.g. ED, clinic, hospitals); and concurrent opioid and benzodiazepine prescription (Minnesota DHS, 2018).

Possible data sources include the Wisconsin Prescription Drug Monitoring Program (PDMP); Green County medical systems, such as the Monroe Clinic; and pharmacies in Green County. It is important to note that police can pull data from the PDMP.

Narcan/Naloxone Use

Naloxone (or Narcan) is an opioid antagonist that can reverse opioid overdoses. It is an important way to prevent deaths due to opioids, and there is evidence that making Naloxone widely available through pharmacies without a prescription, prescribing them to patients and families of patients with opioid use disorders, and having first responders like fire, EMS, and police carry Naloxone are effective at reducing mortality due to opioids (Doyon et al, 2014; Seal et al, 2005).

Metrics include: number and percentage of patients with opioid use disorder prescribed naloxone; quantity of naloxone distributed from pharmacies; number of uses in emergency departments; and number of uses reported in the field from EMS, fire, and police.

Data sources include EMS, police departments, fire departments, emergency departments, and pharmacies. ODMAP could possibly capture this information from several agencies in the field (see ODMAP, Appendix A).

Law Enforcement

Opioid-Related Arrests

Law enforcement plays an important role in response to the opioid crisis. They are often on the front lines of interacting with those who use and distribute drugs like opioids. These interactions could present an opportunity for police to intervene and pursue harm-reduction strategies. Additionally, tracking metrics for law enforcement gives Green County stakeholders a more comprehensive understanding of the opioid crisis as a whole.

Metrics to consider gathering include arrests due to possession of opioids; distribution of opioids; drug seizures; or other crimes (e.g. burglary to obtain opioids). Possible data sources include the County Sheriff and local police departments.

District Attorney

The District Attorney’s (DA) Office also plays an important role in the opioid crisis. They have a unique understanding of the number of opioid users who are processed through the criminal justice system. It’s possible that many opioid users in Green Country interact with the DA, which could present an opportunity for the criminal justice system to intervene and pursue harm reduction strategies.

Metrics to consider gathering include the number of referrals for opioid-related crimes made to the DA each quarter, and the number of those individuals where charges are pursued. Possible data sources include the DA and the DA IT program (PROTECT).

Court System

Drug Courts

Drug courts are specialized court programs that target criminal defendants and offenders, juvenile offenders, and parents with pending child welfare cases who have alcohol and other drug dependency problems (Drug Courts, 2018). Drug courts have become an important harm-reduction criminal justice effort to reduce drug use and recidivism among those with substance use disorders (County Health Rankings & Roadmaps, 2016). Green County has created a drug court program that can be an important asset in fighting the opioid epidemic.

Drug court metrics to consider are the number of opioid-related cases and number of individuals who receive alternative sentencing such as treatment and rehabilitation services. Possible data services include Consolidated Court Automation Programs (CCAP), Substance Abuse Human Services, and Probation, Parole and Law Enforcement.

Benefits of Data Sharing Systems

Developing a data sharing system for a specific issue like opioids can be an incredible asset. However, such a venture also requires a great deal of investment. One should carefully consider both the costs and benefits of sharing data across agencies. Below is a discussion of the benefits of a successful data sharing system.

Improved outcomes

Perhaps the greatest benefit of data sharing systems is the potential to improve outcomes. Data sharing can offer Green County stakeholders more complete knowledge of the local opioid epidemic. Improved understanding in turn creates opportunities for better decision-making processes and high-quality service delivery (Ramon et al, 2007). The strong interorganizational cooperation required to develop and maintain a successful data sharing system can also lead to well-integrated planning and services. All of this will be a boon for meeting opioid users' needs and potentially reducing morbidity and mortality due to opioids.

Having the capacity to identify problems as they develop in real time can be a major asset of data sharing systems for improving outcomes. Integrating timely public health and public safety data is particularly important for confronting the opioid crisis, as several overdoses can occur in a short period of time, especially if a "bad batch" of opioids arrives (Police Executive Research Forum, 2016; Darke et al, 1999). Publicly available data sharing systems like ODMAP that have the capacity to alert agencies when multiple overdoses occur can be an incredible asset (ODMAP, 2018). This capacity could help public health officials mount appropriate responses to prevent future overdoses, such as by alerting other Green County agencies, contacting neighboring counties, or developing a timely PSA.

Increased efficiency and cost savings

Improved efficiency is another advantage of data sharing systems. Because agencies are often siloed, there can be duplicated or even conflicting programs and policies in place by various stakeholders. By collaborating, developing trust, and ultimately sharing data between stakeholders in the opioid crisis, it may be possible to reduce duplicate data collection, processing, and storage activities, thus lowering costs and burdens on staff (Gil-Garcia, Chengalur-Smith, & Duchessi, 2007). Additionally, access to real-time data across multiple systems can make service delivery more efficient, facilitate agencies better allocating resources, and help policymakers to develop appropriate policies and programs (Police Executive Research Forum, 2016).

Data sharing initiatives can also offer cost savings. Especially for conducting research, primary data collection is very time- and resource-intensive compared to integrated administrative data sources (Culhane et al, 2010). Data sharing systems can also reduce the need for costly and frequent data requests, especially for grant applications and community needs assessments.

Increased organizational capacity

The process of developing data sharing systems helps increase organizational capacity. As the involved stakeholders discuss the important opioid-related metrics to measure, definitions and data collection processes can be standardized and technical resources shared (Gil-Garcia, Chengalur-Smith, & Duchessi, 2007). Additionally, data systems facilitate coordination and sharing of knowledge within and between organizations, which strengthens professional networks and promotes collaborative efforts (Police Executive Research Forum, 2016).

Improved grant funding

Importantly, data sharing systems can create opportunities to increase funding levels. Demonstrating to funders that a strong network of organizations and agencies has developed data collection and sharing systems can be major assets. Additionally, agencies often have a short timeframe to apply for grant funding, and data sharing systems can facilitate having access to relevant data in a timely fashion (Gibson, 2018). Any funding can further increase the ability of this collaborative to respond to current and future opioid-related threats in Green County.

Increased interorganizational collaboration

Strong interorganizational collaboration is needed for a successful data sharing system (O’Brien, 2018). Cooperation is maintained through invested leadership, strong social and professional networks, and the sharing of information, strategies, and goals (Gil-Garcia & Sayogo, 2016; Gil-

Garcia, Chengalur-Smith, & Duchessi, 2007; Police Executive Research, 2016). Interorganizational collaboration can also facilitate the effective allocation of resources across the county (Culhane, 2010). Finally, developing data sharing systems specific to opioids can facilitate the sharing of data related to other public health and public safety issues (Gibson, 2018).

Improved accountability

Multi-agency coalitions with the ability to produce important and timely data improves accountability among participating stakeholders. (Gil-Garcia, Chengalur-Smith, & Duchessi, 2007; Police Executive Research Forum, 2016.) Additionally, increased dissemination of stakeholders' achievements as well as their broader program and policy goals can strengthen their reputation in the community. Finally, real-time response to the opioid crisis can provide the means and justification for important PSAs that increase the public's awareness of the collaborative's work and confidence in it.

Barriers

Although there are many benefits of data-sharing systems, potential barriers should be considered prior to implementation. A systematic review of the literature on data sharing in public health found technical, economic, political, and legal barriers commonly mentioned (Panhuis et al, 2014). Below we discuss these barriers in more detail and provide examples that highlight these challenges.

Funding

Creating a data-sharing system is a long-term, large-scale, and resource intensive project. Budgetary allocations will be dependent upon the scale of the data sharing platform proposed. Overall, a large portion of resources will be needed for the early stages of developing a data sharing system. The Milwaukee DataShare and Cardiff Model will serve as examples for this section (Downey & Olson, 2013).

As an example, the Milwaukee DataShare group budgeted nearly $300,000 to collect opioid-related data and add it to their existing integrated data system (IDS) over a 30-month period. In comparison, Green County's budget for a data sharing platform will be considerably lower, but would still demand a large number of resources for development. (Milwaukee Data Share, 2018).

Initial funding areas

With data-sharing projects, initial costs are typically considerably higher than long-term maintenance costs. There are three major priorities to consider: data management, sharing data, and analyzing and disseminating your findings. Understanding each of these three areas will help with developing a proper budget for the data sharing platform (Pisani & AbouZahr, 2010).

Data Management

Data management is a very important aspect to consider. The policies implemented around data management will define the quality of your data library (i.e. accessibility, user friendly, understandable, etc.). Initial steps will include compiling datasets from all agencies involved into one data library, which undoubtedly will mean converting multiple data libraries into one cohesive library. Metaphorically speaking it will be like converting agency specific reports from a French, Italian, and Spanish into English. Your data will need to undergo a similar translation process in order to fit into the data platform. The data analyst responsible for this task will also be responsible for managing the data library after it has been developed as well as continuously inputting new data in the correct form (Pisani & AbouZhar, 2010; Downey & Olson, 2013).

Developing metadata standards is also an area worth noting. Agencies involved in this data sharing platform will need to adhere to strict data collection, management, and dissemination methods in order to maintain long term ease of accessibility. Going back to the language example, agencies cannot continue creating reports in Spanish, French, Italian, or whichever language they prefer. After becoming a part of the data sharing platform, they will need to adhere to creating reports in English, or the format that is best preferred by the data sharing platform. This may result in budgetary demands to upgrade computers, data collection methods, and other areas. It is important to create a foundation that will maintain your data for long term use with minimal future improvements to avoid more spending costs (Downey & Olson, 2013).

Sharing Data

Data sharing is no easy task and will require coordination by all agencies. A data analyst and/or data manager, as mentioned previously, is an investment that should be considered. Not only will the data analyst be responsible for managing the dataset and inputting new information, he/she will also serve as a resource or expert to answer any data related questions related to the platform (Panhuis, 2014). Understanding the data that will be shared amongst agencies is very important for proper utilization of this program. The analyst will also be responsible for holding training and informational sessions related to data collection, data standards, and all data policies related to the data sharing platform to best educate participants on the data sharing arrangement (Panhuis, 2014).

Policies will need to be drafted in order to make the sharing of data cohesive and secure. More will be discussed regarding the security of data in a section further in the report. Cohesiveness of data sharing will also need to be a priority and will bring many challenges. Understanding past policies in data collection will be important in creating new policies. It is important to document and detail past procedures and collection methods to disseminate amongst agencies to overcome many of the challenges that come with data conversion and sharing that will impact future analyses and recommendations. For example, gaps in data collection will need explanation. Was this information mistakenly omitted, has it not been inputted, and should we continue to collect this information in the future? These are all kinds of analytical questions that agencies will need to ask themselves when reviewing data for the platform.

Data Analysis

Data analysis is an important area that will need budget allocations and will ultimately facilitate motivation by the agencies involved (Panhuis, 2014). Quarterly, bi-annual, and/or annual reports will provide the agencies involved an understanding of their investment into the data sharing platform. Data analyses should also be utilized as incentives for agencies to participate in the data sharing platform through predetermined expectations on how agencies will utilize the accessible data.

Issues to Consider

The ultimate issue to consider is how to acquire the necessary funding for initial startup costs, specifically, who will take on the responsibility to acquire these funds. This is another area that will need to be considered by the committee when outlining the timeline for this project. Funding is an important aspect for the success of this data sharing platform and the committee will need to recognize an individual or group of individuals who will be responsible for funds.

Public health has limited availability to funding and other necessary resources and is an obvious barrier for many projects. With the opioid crisis affecting many communities throughout the nation, grants and other funding are easier to come by. State health departments and federal health agencies are working full force to understand and combat the opioid crisis. Collaboration amongst communities, big or small, is the key to containing the effects and getting help for the individuals that need it the most.

How to Address Issues

There are two major ways of classifying fundraising efforts: internal revenue and external revenue. Grants (external revenue) will be an important catalyst for the development of this data sharing platform and will require continued efforts to seek out and apply for new grants. Internal revenue should also be considered by Green County. What is meant by internal revenue is to generate a portion of the funds through participating agencies by having them pay a small portion to be included into the data sharing platform, or to gain access to certain aspects of the data sharing platform. Their buy-in will incentivize collaboration and utilization of the data library.

The initial costs will be much higher than the long-term maintenance costs, which means a short-term grant may be able to cover the starting costs. Bob Gibson has already initiated work in this area by applying for a grant funded by the Division of Public Health in the Wisconsin Department of Health Services. The grant is awarding public health crisis response funding to Local Public Health Agencies, Health Emergency Readiness Coalitions, Tribal Health Centers, and Regional Trauma Advisory Councils to work to strengthen public health preparedness and response around the ongoing opioid overdose epidemic in Wisconsin (Gibson, 2018).

Maintenance Funding

Maintaining a data sharing platform requires fewer financial resources than the initial startup costs, but should not be neglected. Technology is continuously upgrading and becoming increasingly sophisticated, providing users with high-tech tools that can be utilized more efficiently in their daily lives. Data sharing platforms are constantly undergoing upgrades, which will affect current data standards and policies. These policies will need to be updated with upgrades and should be evaluated by a data specialist.

Issues to Consider

Even though maintenance costs will remain relatively low, agencies will need to consider intermittent and required modifications to the platform. Technology is constantly changing and evolving to benefit research and the data library, and it is necessary to continue integrating new updates to old systems. This will allow for future expansion and reduce the need to develop a completely new platform every few years, which would result in large sums of financial resources spent.

How to Address Issues

To address these issues, it is recommended that the agencies involved develop a set of specific goals the data sharing platform will achieve as well as a timeline of necessary updates the platform will undergo. This should be integrated into the budget plans for the project. A financial expert and data experts will need to be consulted for a precise development of goals related to the data library and the financial resources needed for the project.

Technical Barriers

Perceived hardware and software complexity are often cited as barriers to implementing a data sharing system (Gil-Garcia, Chengalur-Smith, & Duchessi, 2007). When developing a data sharing system, choosing a platform that will allow you to communicate your data effectively is critical to the success of the system. The following section will discuss the technical limitations of the previously mentioned data sharing systems and provide examples of existing systems addressing these technical challenges (see Appendix A). Finally, this section will examine the importance of internal and external data security.

System Structure

Issues to Consider

Regardless of the system structure, there are many common technical barriers that can decrease the functionality of the data sharing system (Gil-Garcia, Chengalur-Smith, & Duchessi, 2007). As previously mentioned with HIE, if the information is not being collected or the system is not capable of recording the metrics of interest, it may require more technical resources than anticipated to incorporate and share this information (Fontaine et al, 2010). When the data is stored in different formats within each organization it can also be more difficult to combine and share data. Even if the data is stored in the same format, extracting, cleaning, and importing data between systems can be time consuming and inefficient (Police Executive Research Forum, 2016). Once the system has been implemented, there may be a delay between information in the system and information in reality.

How to Address Issues

Although technical barriers are common, many existing data sharing systems have found ways to address these problems. When the Cardiff Model was developed, they worked with Epic IT professionals to create new sections in the patient's medical records when they discovered that certain metrics of interest were not being collected in the existing Electronic Health Record (EHR). They also worked closely with nurses and physicians to ensure they were willing and able to collect and input this new information into the chart when patients were seen in the ED. They emphasized the importance of nurse and physician champions in gaining acceptance and increasing understanding of the opioid crisis as a public health issue. Additionally, ODMAP is tool specifically designed for the opioid epidemic and provides a platform for collecting and storing opioid metrics, if they are not already being collected (ODMAP, 2018).

In the Cardiff Model, EMS and police officers were able to continue to collect data in their original systems. On a monthly basis, they extracted the relevant data from their system and sent it to a data analyst, allowing them to avoid the common issue of incompatible data formatting. While extracting, cleaning, and importing data between systems can be time consuming, many existing data sharing systems rely on the use of a research or administrative assistant. The Cardiff Model hired a part time research assistant to extract, de-identify, and consolidate the data to be sent to the data analyst on a monthly basis. The Camden Coalition hired a similar assistant who was in charge of overseeing the data extraction and analysis process. Additionally, the Camden Coalition recommends hiring an IT professional who has worked on a similar system previously to help address any further issues that may arise during the process of implementing the data sharing system. Finally, ODMAP is one of the only systems that allows for data collection in real-time to address the delay between data in the system and in reality (Darke et al, 1999).

Security

When information is aggregated and shared between different organizations, there is a risk of the data being accessed and used inappropriately. The use of internal and external security measures can decrease the threat to system security. This section examines potential security threats and provides examples of protective measures.

Issues to Consider

Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, organizations must assess the vulnerability of electronic protected health information (PHI) and establish appropriate safeguards to ensure the confidentiality of the protected information (HHS Office, 2013). When data is accessible by multiple users, such as in a data dashboard, the data can be misused which threatens data security internally (Rosenfeld et al, 2007). Users may access the information outside of a secure facility or access information beyond the scope of their work (Henry M., 2015). Additionally, data security may be threatened externally when information is stored or shared between organizations.

How to Address Issues

The HIPAA Security Rule recommends multiple measures to protect the internal and external security of electronic PHI (ODMAP, 2018). The recommendations include controlling access, monitoring activity in the system, integrity controls to ensure the information is not altered or destroyed, and transmission security to protect against unauthorized access (ODMAP, 2018). ODMAP protects the information stored electronically by having different levels of users with different access to the data (Darke et al, 1999). Level 1 users enter data into the system without identifying information. Level II users are required to use a password and have access to all information collected by the level I users. Similarly, ArcGIS has level 1 and level 2 users with strict guidelines over who can view the data.

In the Cardiff Model system, only the data analyst has access to the de-identified information. This system does allow you to zoom in on the map to see an exact location of assaults, but this information is not available to the public. With data dashboards, where multiple users may be entering and analyzing the data, passwords are often utilized to guarantee the internal security of the information. Additionally, hardware, software, and procedural mechanisms can be used to protect against external threats to data security (Human Services, 2013).

Organizational Culture as a Barrier to IDS Implementation

The data sharing platform will be shared amongst multiple agencies requiring policies and standards developed around the data library that will be agreed upon by all participants. Not only will this create more work, but may also result in pushback by many participants. Flexibility will be necessary to overcome many of the cultural and organizational barriers that will be discussed in this section.

Issues to Consider

Many organizational and cultural barriers present themselves in the form of motivations in the data sharing context (Panhuis, 2014). Data sharing requires a lot of time and resources, both of which are lacking in the public sector. This results in an opportunity cost for all agencies who will participate in the data sharing platform (Pisani & AbouZahr, 2010).

A second organizational barrier that will present itself is the consensus on data use agreements. Data is a very valuable asset for any agency or institution and requires monitoring of how it will be used and who will have access to it. Misuse of data is an area of concern when it involves sensitive information like medical data and legality of sharing such information. This topic was previously touched on in the 'Security Barriers' section and will be further covered below in the 'Legal Barriers'. Defining parameters that the participants are comfortable with will be a challenging task, but a necessary part of a successful data sharing agreement.

How to Address Issues

Personal and institutional incentives will be the key to addressing the issues mentioned above. Many data sharing platforms have utilized an enrollment fee to increase incentives. Agencies are required to pay a small fee in order to gain access to the data sharing platform. This will help with the maintenance costs mentioned in the previous section as well as ensure utilization of the data library. The small fee will also entitle agencies involvement in the development of a data agreement.

Developing a data agreement will need to be seriously considered by all participants. Examples of data agreements can be found in Appendix B. This agreement will be a key foundational piece to build trust between the agencies involved in the data sharing platform. This agreement will also facilitate an agreement on the standards that agencies should adhere to when collecting, transferring, inputting, and managing their data.

Misuse of shared data will also need to be addressed by a data agreement. As stated previously data is very sensitive and valuable with a lot of responsibility attributed. Agencies need to be comfortable sharing their data amongst other agencies. Data agreements must define what activities would be considered misusing data. Resources will have to be made available to participants who have further questions for clarifications. A protocol for handling cases of data misuse will need to be developed as well (Panhuis, 2014; Downey & Olson, 2013).

Political and Cultural Barriers

Other than the overall apprehensive nature of sharing data between agencies due to the possibility of data misuse there will be other political and bureaucratic barriers to consider. Barriers have been embedded into the public health system due to the governance framework grounded in a political or socio-cultural context.

Issues to Consider
Agencies may have implemented specific policies that may restrict the use and sharing of data. This is a barrier that will define the extent of the data sharing platform and will also affect the coalition's decision on their sources of data. Furthermore, inconsistencies in policies regarding data sharing will create constraints and will need to be considered when developing data agreements.

How to Address Issues
It is important to understand each agency's data-sharing policies and constraints before moving forward with building the data-sharing platform. This barrier will be the limiting factor that will define your data library. If data related policies are too constraining it may be an indication to utilize other sources like data collected by the Department of Health Services, County Health Rankings, and the Department of Public Health.

Legal Barriers

Legal barriers are also commonly cited as a challenge to sharing information between organizations. However, the laws protecting health information are often misunderstood, which leads practitioners to assume the laws are more restrictive than the regulation requires. Generally, these laws are meant to provide guidance about the conditions in which PHI can be shared.

While there are many laws protecting health information, Health Insurance Portability and Accountability Act of 1996 (HIPAA), is considered one of the most important barriers to exchanging health information. Additionally, unique real and perceived legal challenges arise when collaborating between the criminal justice system, mental health, and substance abuse treatment programs regarding the sharing of individual information. Substance abuse treatment information is protected under 42 CFR Part 2, a portion of the Code of Federal Regulations (Petrila & Fader-Towe, 2010).

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Issues to Consider

HIPAA establishes federal standards for privacy and security of PHI (Summary of HIPAA, 2013). The Privacy Rule under HIPAA addresses the use and disclosure of individual PHI and applies to healthcare providers, health plans, and healthcare clearinghouses (Summary of HIPAA, 2013). The Privacy Rule protects all individually identifiable health information, such as name, date of birth, address, and social security number (Summary of HIPAA, 2013). Information covered under the Privacy Rule may not be disclosed unless written authorization from the subject of the information is obtained (Summary of HIPAA, 2013).

How to Address Issues

However, obtaining authorization for the use of PHI can be challenging and inconvenient, so de-identifying individual information is often the preferred method for using health information. The use and disclosure of de-identified information does not apply to the restrictions under HIPAA. To de-identify PHI, the specific individual identifiers listed above must be removed. Additionally, the Privacy Rule permits the use of PHI without individual authorization if the information is to be shared for the purposes of treatment, payment, or health care operations activities. Health information may also be shared as required by law and in judicial orders.

Many existing data sharing systems have overcome legal barriers, such as those outlined above. The Cardiff Model uses de-identified health information to track trends in the opioid metrics of interest. As previously mentioned, a research assistant was hired to collect information from the EMR, de-identify the information, and send the data to the data analyst. In this example, only one member of the research team has access to PHI. The Minnesota Dashboard avoids this issue by only using aggregated data that has previously been de-identified in their dashboard.

42 CFR Part 2

Issues to Consider

42 CFR Part 2 is part of the Code of Federal Regulations that is concerned with the confidentiality of alcohol and drug abuse patient records and applies to all federally assisted programs (Summary of HIPAA, 2013). While HIPAA does include mental health information, 42 CFT Part 2 tends to be more restrictive in the information that can be shared. 42 CFT Part 2 requires consent in many cases of PHI excluding emergencies, court order, and other specific provisions (Summary of HIPAA, 2013).

How to Address

Law enforcement officials are not covered under HIPAA or 42 CFR Part 2. Thus, if an officer learns of an individual’s substance abuse or mental health condition, they are allowed to share this information and include it in a report, if applicable. Additionally, 42 CFR Part 2 does not require drug court hearings to be closed. However, when information is disclosed in a court order, Part 2 requires that steps be taken to protect patient confidentiality (Angie, 2013).

Other Legislative and Regulatory Considerations

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 provided federal funding for health information technology. The HITECH act provided incentives to physicians and hospitals to implement EHRs (Mennemeyer et al, 2016). Under HITECH, business associates must comply with the provisions of HIPAA. Business associates are entities that perform activities that involve the use or disclosure of PHI for a covered entity, such as providing legal advice or claims processing.

There are many other laws that govern the sharing of information, often at the state level, that should also be considered when developing a data sharing system. Creating legal documents and consulting with legal counsel in the process of system development can be useful for addressing these barriers.

Key Considerations in Creating Data Sharing System

When developing a data sharing system, the previously mentioned barriers should be taken into consideration. Developing data sharing agreements or memoranda of understanding (MOUs) can address multiple barriers and facilitate discussions around the use of the data. The following section further discusses the importance of these documents.

Data Sharing Agreements and Memoranda of Understanding

Data sharing agreements or memoranda of understanding are documents reflecting an agreement between two parties (Developing Data Sharing Agreements, 2018). Ideally, these documents should be developed and signed before the implementation of the data sharing system, providing the foundation for the rest of the project. These documents should involve stakeholder participation and focus on addressing concerns and building trust between the organizations. Throughout the process of implementation, partners can refer to the agreements for guidance on the continuation of the project.

Additionally, data sharing agreements can help to address the technical, organizational, political, and legal barriers previously discussed. Most data sharing agreements discuss what data will be shared, how and with whom the data will be shared, and how data will be kept secure. The process of developing the data sharing agreements will establish open communication between partners to ensure success of the data sharing system.

We have included examples of data-sharing agreements or memoranda of understandings in Appendix B.

Recommendations

Developing a data-sharing system in Green County is possible by taking into consideration the previously mentioned barriers. Based on our discussions with community members from Green County, they have been collecting relevant data within each agency. Future directions should involve increasing collaboration with additional stakeholders, addressing challenges with system structure and security, and establishing appropriate legal frameworks to facilitate the sharing of data within each agency. Addressing these financial, technical, legal, and organization barriers will allow Green County to develop a data sharing system to combat the opioid crisis.

Short Term (High Priority)

Establish a coalition for data sharing
Initially, when developing a data-sharing system, it is important to consider the coalition or organization that will be responsible for the system. This organization will apply for grants to obtain funding for the system, will hire the necessary technical and administrative assistants, and be in charge of managing data and generating reports. The Criminal Justice Coordinating Council or the Green County Healthy Community Coalition may be chosen as this organization, but important organization barriers mentioned above should be considered prior to this decision.

Engage stakeholders
Engaging with stakeholders early and often will be crucial to the success of the data sharing system. For example, discussions with stakeholders in healthcare and law enforcement about their role in the system can help to begin addressing funding and legal barriers for sharing data. These discussions should include the type of data shared, the type of agreements necessary, and the cost for obtaining this data. Additionally, establishing connections with IT professionals about the potential for adding any novel metrics to existing data collection systems will be helpful for the rest of the project. Finally, it will be important to decide if the general public will have access to results or reports from this data sharing system, or if it will remain an internal document among participating stakeholders.

Begin discussing system structure
While it is not necessary to finalize the system that will be used in the early stages of program planning, it is important to start thinking about the larger implications for each of the different system structures. One of these larger considerations is the purpose of the data-sharing system. Specifically, considering whether the data will be used for real time response, long term prevention, or both. ODMAP is a tool that allows for real time response and is an easy tool to begin using as soon as possible. If the goal is long term prevention and obtaining funding for future projects, an aggregated data system may be more beneficial.

Another important consideration at this stage is the decision to use aggregated de-identified data or individual-level data. Discussing available data with the Department of Health Services (DHS) could be useful in making this decision. They provide aggregated, de-identified data at the county level and it may be relevant to include in the system.

Identify funding needs

Once the goals for the project have been established, it is important to consider a budget for system development and maintenance of the system. This report has provided some guidelines for certain costs, but discussing further with stakeholders such as healthcare organizations, law enforcement, and IT professionals will allow for a more thorough budget to be developed.

Mid Term (Medium Priority)

Apply for grants and other funding sources

Once the committee has identified the funding needed for the project and created a detailed budget, applying for grants and identifying other funding sources will be a priority. When applying for grants, seeking out those that are long-term, renewable, and align with the data sharing coalition's goals and vision are important areas to consider. It will also be useful to consider the data source used for this data sharing platform. Using individual level data will give you richer data, but will require more translation and clean-up. Data available by the state or other sources will require less cleaning, but will not be as rich and meaningful for the coalition's goals.

Long-term grants will reduce the frequency of applying for grants and the same goes for those that are renewable. Applying for grants that align with the goals outlined by the coalition will also create efficiency and reduce opportunity cost associated with grant writing.

Finalize Metrics with Committee

To make data collection more efficient your committee members will need to finalize a list of opioid-related metrics that will be included in the data sharing platform. A list of metrics can be found in the 'Opioid-Related Metrics' section. As discussed previously, including a greater number of metrics in the data-sharing platform will increase the richness of the data, the number of stakeholders involved in this project, and the complexity and cost of this data sharing venture.

Decide on Data Sources

Deciding which data sources to use for the data sharing platform is a crucial step and will affect the efficiency and longevity of your aggregate data. This decision will also affect the type of data sharing agreements that will be drafted. There are ultimately two options for the source of your data: county-level data that stakeholders in your coalition will collect or state level data.

Collection of data by members of the coalition will require more resources, but will provide very rich and applicable data. Data collection, inputting data, and management of the data will require training of individuals and many policies to be implemented and adhered to.

Using data provided by Department of Health Services (DHS) will require fewer resources, but could be outdated, not as representative of Green County, and will limit the types of analyses that can be conducted. However, it may be possible to receive Syndromic or rapid response data (hospital data reported to DHS) on a more frequent basis from the DHS. The coalition should reach out to DHS about the possibility of receiving such reports and determine whether this would meet the coalition's needs.

It may soon be possible to get state-level criminal justice data. The state-wide Criminal Justice Coordinating Council (CJCC) is considering compiling data for all individuals in Wisconsin who have been processed through the criminal justice system. This system would include individual level data from prosecution, courts, and jails; however, it is unlikely to include health-related data from DHS due to HIPAA constraints. While this information would not be specific to opioid users, it may be possible to filter through the data and search for individuals with opioid charges or convictions. The coalition can follow up about this data in the CJCC coordinators meetings.

Ultimately, using data from state agencies will be much less costly, but the data may not fully meet the needs of this data sharing initiative. Your data source decision will likely be affected by the amount of funding available.

Choose Data-Sharing Software

After finalizing the data-sharing system structure, metrics, and data sources, the coalition will have the necessary information to choose an appropriate data-sharing software. Examples of software specific to various types of data sharing systems have been provided in the 'Types of Data-Sharing Systems' section. However, it should be noted that the examples provided are not comprehensive and the coalition should perform their own investigation of potential software that could best meet their needs.

Different software will require distinct skills and knowledge to manage. For example, *RStudio* is a free software with the capacity to create tables and figures for a dashboard, but requires experience with the *R* programming language. The coalition should keep this in mind when considering hiring IT professionals to support this data-sharing system (see below).

Developing Data-Sharing Agreements

To address the sensitive nature of sharing confidential data, a formal contract should be devised. This contract should clearly identify what data will be shared and how it can and cannot be used. A data-sharing agreement will protect the agencies providing data by ensuring that data will not be misused. Secondly, the data share agreement will prevent miscommunication regarding the use of the data by both the data providers and receivers. This document will promote collaboration and discussion regarding data use that has not been documented previously. New data use issues and understandings should then be documented and included in a revised data share agreement for future use.

A separate data share agreement should be drafted for the creation of the ODMAP, if the coalition decides to implement this recommendation.

Consider hiring IT professional, administrative assistant
Creating a data-sharing platform is going to require knowledge and skills related to software development, data management, and administrative skills. It is recommended that a professional software developer be hired to develop the data-sharing platform. An administrative assistant dedicated to this project should also be considered depending on funding options. Both of these positions will be important in development and management of the data platform as well as adhering to a specific timeline.

Create evaluation plan
Evaluation plans should be outlined early in program development. Your evaluation plan should include formative and outcome evaluation using both qualitative and quantitative data. Determining the degree to which your program goals and policies are being met is important to share with all stakeholders in order to improve decision-making related to the data-sharing platform. Your evaluation design should be flexible enough to assess intermediate changes in opioid related metrics. Evaluations should also include an analysis of long term goals specified by the committee. These goals will steer the potential of the data-sharing platform and should be remodeled over time.

Long Term (Low Priority)

Begin gathering data on new metrics
To minimize burden on participating stakeholders, this initiative should avoid requesting that agencies gather any new information or metrics that they weren’t previously recording. However, if there are data that this collaborative believes are vital to its success and functioning, then exceptions can be made.

It will likely take months or years to begin gathering data about any new metrics. Novel data collection and storage processes will need to be developed, and it will also take time to generate buy-in from staff whose workflows may change. We recommend networking with other jurisdictions in Wisconsin to see if other agencies gather new metrics of interest, and if it is possible to replicate their data collection methods. This will save valuable time, energy, and resources.

Share data, input data into software, create reports

After Green County stakeholders decide which metrics and data to share, buy the software that will compile data, and hire any necessary IT professionals, it will be time to begin the actual data sharing. Data should be sent securely to the agency in charge of managing the data, specifically to a HIPAA compliant server if working with protected health information. Data will be inputted into the software, and reports can be generated.

It is likely that some stakeholders will lag behind others in gathering data and finalizing data-sharing agreements. We recommend that this collaborative begins sharing data once any stakeholders are ready to do so and the infrastructure exists to receive the data - even if other stakeholders are not prepared to share their data. Reports may be quite valuable even if the data available is incomplete. There will also be a steep learning curve for sharing, compiling, and analyzing the data, so getting practice in these processes sooner rather than later will be valuable experience.

Share results with stakeholders

Once data have been processed, it is time to share the results with stakeholders. Data and results will be provided to stakeholders according to the data-sharing agreements that were previously developed. Depending on the terms of the agreement and type of data-sharing system created, results may be shared in real-time and on an ongoing basis, or at regular intervals (e.g. monthly or quarterly). The coalition may also share results with the general public to promote accountability, depending on the sensitivity of the data and goals of the initiative.

Utilize for prevention efforts

This data-sharing system should offer stakeholders in Green County a more complete understanding of the local opioid epidemic. The coalition managing the data-sharing initiative should meet on a regular basis to analyze and discuss reports to see where there may be previously undiscovered needs related to opioids or opportunities to intervene. Thus, the data can guide local program and policies and assist in evaluating the impact of such interventions.

Utilize dashboard to apply for grant funding

The data-sharing system will present opportunities to apply for grant funding. Stakeholders will have access to timely data from a variety of agencies, which can be utilized in grant applications. By employing data from and highlighting the strengths of this data-sharing system, Green Country will be more competitive for grant funding and can use new funding to develop programs that better meet the needs of opioid users.

Conclusion

There are multiple stakeholders involved in the opioid epidemic, including law enforcement, courts, jails, healthcare, and EMS. Each of these stakeholders' perspective is crucial to understanding the broad factors contributing to and driving this opioid use which is why data sharing is an important component to facilitate collaboration. In this report, our team has identified the benefits of a data-sharing platform, key barriers and challenges that will arise while developing this platform, and a strategic timeline of recommendations outlined by level of priority for Green County to focus on as they move forward.

References

Angie, Rich. (2013, July 15). Confidentiality Regulations FAQs. Retrieved November 20, 2018, from https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs

Coffin, P. O., Tracy, M., Bucciarelli, A., Ompad, D. C., Vlahov, D., & Galea, S. (2007). Identifying injection drug users at risk of overdose.

County Health Rankings & Roadmaps. (2016, October 19). Retrieved November 20, 2018, from http://www.countyhealthrankings.org/take-action-to-improve-health/what-works-for-health/policies/drug-courts

Culhane, D. P., Fantuzzo, J., Rouse, H. L., Tam, V., & Lukens, J. (2010). Connecting the dots: The promise of integrated data systems for policy analysis and systems reform.

Darke, S., Hall, W., Weatherburn, D., & Lind, B. (1999). Fluctuations in heroin purity and the incidence of fatal heroin overdose. *Drug and Alcohol Dependence*, *54*(2), 155-161.

Developing Data Sharing Agreements. (2018). Retrieved November 20, 2018, from http://rpp.wtgrantfoundation.org/developing-data-sharing-agreements

Downey, A. S., & Olson, S. (Eds.). (2013). *Sharing clinical research data: workshop summary*. National Academies Press.

Doyon, S., Aks, S. E., & Schaeffer, S. (2014). Expanding access to naloxone in the United States. *Journal of Medical Toxicology*, *10*(4), 431-434.

Drug Courts. (2018). Retrieved November 20, 2018, from https://www.nij.gov/topics/courts/drug-courts/Pages/welcome.aspx

Fontaine, P., Ross, S. E., Zink, T., & Schilling, L. M. (2010). Systematic review of health information exchange in primary care practices. *The Journal of the American Board of Family Medicine*, *23*(5), 655-670.

Gibson, B. (2018, September 25). Virtual Interview.

Gibson, B. (2018, October 11). Virtual Interview.

Gil-Garcia, J. R., & Sayogo, D. S. (2016). Government inter-organizational information sharing initiatives: Understanding the main determinants of success. *Government Information Quarterly*, *33*(3), 572-582.

Health Information Exchange. (2018). Retrieved November 20, 2018, from https://www.healthit.gov/topic/health-it-basics/health-information-exchange

Henry M. Toolkit for Communities Using Health Data. *National Committee on Vital and Health Statistics*. [PDF file]. Retrieved from https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/Toolkit-for-Communities.pdf. Published May 2015.

HHS Office of the Secretary, Office for Civil Rights, & OCR. (2013, July 26). Summary of the HIPAA Security Rule. Retrieved November 20, 2018, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Human Services - 2013 Sustained and Coordinated Efforts Could Facilitate Data-Sharing While Protecting Privacy. *United States Government Accountability Office*. [PDF file]. Retrieved from: https://www.gao.gov/assets/660/652058.pdf

Hofman, W., & Rajagopal, M. (2014). A technical framework for data sharing. *Journal of theoretical and applied electronic commerce research*, *9*(3), 45-58.

Integrated Data Systems (IDS). (2018). Retrieved November 20, 2018, from https://www.aisp.upenn.edu/integrated-data-systems/

Kolodny, A., Courtwright, D. T., Hwang, C. S., Kreiner, P., Eadie, J. L., Clark, T. W., & Alexander, G. C. (2015). The prescription opioid and heroin crisis: a public health approach to an epidemic of addiction.*Annual review of public health*, *36*, 559-574.

Martell, B. A., o'Connor, P. G., Kerns, R. D., Becker, W. C., Morales, K. H., Kosten, T. R., & Fiellin, D. A. (2007). Systematic review: opioid treatment for chronic back pain: prevalence, efficacy, and association with addiction. *Annals of internal medicine*, *146*(2), 116-127.

Massachusetts Department of Public Health (2016). The Massachusetts Opioid Epidemic: A Data visualization of Findings from the Chapter 55 Report. Retrieved November 20, 2018, from https://chapter55.digital.mass.gov/

Medical College of Wisconsin (2016). Advancing a Healthier Wisconsin backs multi-agency project to share opioid data. Retrieved from: https://urbanmilwaukee.com/pressrelease/advancing-a-healthier-wisconsin-backs-multi-agency-project-to-share-opioid-data/

Mennemeyer, S. T., Menachemi, N., Rahurkar, S., & Ford, E. W. (2016). Impact of the HITECH act on physicians' adoption of electronic health records. *Journal of the American Medical Informatics Association*, *23*(2), 375-379..

Milwaukee, WI: Data Share. (2018). Retrieved November 20, 2018, from https://www.aisp.upenn.edu/network-site/milwaukee-data-share/

Minnesota Department of Health. (2018). Minnesota Deparment of Health. Retrieved November 20, 2018, from http://www.health.state.mn.us/divs/healthimprovement/opioid-dashboard/

ODMAP. (2018). Retrieved November 20, 2018, from http://www.hidta.org/odmap/

O'Brien, M. (2018, November 5). Phone Interview.

O'Brien, M. Notes from the Field: Opioid Crisis Understanding the Opioid Crisis Through Data and All-Stakeholder Reviews. Retrieved from: https://www.nij.gov/publications/Pages/notes-from-the-field-opioid-epidemic-obrien.aspx

Panhuis WGV, Paul P, Emerson C, et al. A systematic review of barriers to data sharing in public health. *BMC Public Health*. 2014;14(1). doi:10.1186/1471-2458-14-1144.

Petrila, J., & Fader-Towe, H. (2010). *Information Sharing in Criminal Justice-mental Health Collaborations: Working with HIPPA and Other Privacy Laws*. BJA. *33.*

Pisani, E., & AbouZahr, C. (2010). Sharing health data: good intentions are not enough. *Bulletin of the World Health Organization*, *88*, 462-466.

Police Executive Research Forum. 2016. *Building Successful Partnerships between Law Enforcement and Public Health Agencies to Address Opioid Use*. [PDF file]. Retrieved from: https://ric-zai-inc.com/Publications/cops-p356-pub.pdf

Priorities - Green County Healthy Community Coalition. (2018). Retrieved November 5, 2018, from https://www.greencohcc.org/priorities/

Ramon Gil-Garcia, J., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector. *European Journal of Information Systems*, *16*(2), 121-133.

Rose, A. J., Bernson, D., Chui, K. K. H., Land, T., Walley, A. Y., LaRochelle, M. R., ... & Stopka, T. J. (2018). Potentially Inappropriate Opioid Prescribing, Overdose, and Mortality in Massachusetts, 2011–2015. *Journal of General Internal Medicine*, 1-8.

Rosenfeld, S., Koss, S., & Siler, S. (2007). *Privacy, security, and the regional health information organization*. California HealthCare Foundation.

Seal, K. H., Thawley, R., Gee, L., Bamberger, J., Kral, A. H., Ciccarone, D., ... & Edlin, B. R. (2005). Naloxone distribution and cardiopulmonary resuscitation training for injection drug users to prevent heroin overdose death: a pilot intervention study. *Journal of Urban Health, 82*(2), 303-311.

Washtenaw County Health Department (2018). August 2018 Washtenaw County Opioid Report. Retrieved November 8, 2018, from https://www.washtenaw.org/opioids

Wisconsin Department of Health Services; Division of Public Health (2017). *Select Opioid-Related Morbidity and Mortality Data - November 2016*. [online] Available at: https://www.dhs.wisconsin.gov/publications/p01690.pdf [Accessed 5 Nov. 2018].

APPENDICES

Appendix A: Examples of Data Sharing Initiatives

DataShare

DataShare is a Milwaukee-based initiative that has developed a far-reaching integrated data system. DataShare was originally created to address gun violence and criminal justice in Milwaukee by linking data between several agencies that could provide insights on how to address these issues (O’Brien, 2018). DataShare has connected data from stakeholders such as law enforcement, corrections, courts, prosecution, healthcare, and schools. As the opioid epidemic has grown, Data Share helped found the Unscrambling Data for Urban and Rural Opioid Resiliency project to bring in new agencies that could provide data to address the opioid issue. This includes EMS, medical examiners, Milwaukee Health Department, and prescription drug monitoring programs (PDMPs).

Data Share is a classic integrated data system in that it links individual data between all of these different agencies. This allows its analysts “to create an illustration of an individual’s journey through public services. The path will be linked with waypoints that may show the various steps within a journey taken by someone using opioids, from an Emergency Department visit through multiple support systems and possibly the criminal justice system. By analyzing the journey taken, agencies can develop strategies to redirect the path of patients on a similar trajectory” (Medical College of Wisconsin, 2016). This data system is supplemented with all-stakeholder reviews of overdose fatality cases that aim to identify system weaknesses that could have contributed to a fatality.

It took approximately 6 months to create the Data Use Agreements for agencies sharing medical data related to opioids. However, Dr. O’Brien stressed that they already had much infrastructure in place through their existing integrated data sharing system. They also were already partnering and had developed relationships with some of the agencies that provided opioid data. If this were not the case, it would likely have taken much longer.

The costs for adding the opioid data to the existing DataShare system was nearly $300,000. These costs covered data integration, analysis, and storage for 2.5 years, though mostly covers staff costs. However, these expenses were with a lot of infrastructure already in place, and so it would have likely cost more if they were starting from scratch.

Given the variety of stakeholders involved in DataShare, it encourages a multi-agency response to the opioid epidemic and breaking out of traditional silos. Data Share is currently developing a dashboard for overdose reviews, which will visualize data including overdose locations, the demographic information of individuals who have overdosed, and the hospital destination of those who overdose.

There are privacy concerns and barriers with DataShare, given that the initiative receives data sets with identifying information. After identified data is received, the data is linked with that of other agencies and then de-identified. After de-identification, the information is viewed in aggregate. The agencies that provide information to DataShare have created data sharing agreements and Memoranda of Understanding to outline what information they share and also what data those agencies can receive from DataShare. Data is de-identified for data requests, except when identifying information is required for prevention purposes. Data is stored in a location that is HIPAA and FERPA compliant. Traffic is monitored securely on servers and can be accessed only through a secure portal. Only a select few data managers have access to identifying information.

To minimize creating extra work for stakeholders, DataShare has tried to build upon the data that each agency is already collecting. They have not added new instruments or data collection methods that they view would be burdensome for agencies and possibly reduce participation.

Dr. O'Brien also noted that there were other barriers to the sharing data among agencies. Sometimes unexpected information arises from the data that may portray an agency's work in a negative light. This can cause agencies to lose interest in participation or withdraw completely. She stressed the importance of having regular meetings with stakeholders where agencies can develop shared goals and values to address these types of issues.

Contact information relevant to Data Share:
Dr. Mallory O'Brien; Assistant Professor, Medical College of Wisconsin; Founding Director of Milwaukee Homicide Review Commission and Data Share: mobrien@mcw.edu
Dr. William Hauser, Senior Research Analyst, Wisconsin Department of Justice: hauserwj@doj.state.wi.us

ODMAP

ODMAP is a map-based data-sharing system. ODMAP is a program developed by the High Intensity Drug Trafficking Areas federal program administered by the White House Office of National Drug Control Policy. ODMAP is a national data-sharing tool that provides real-time overdose surveillance data across jurisdictions. This was developed to support public safety and health efforts, as well as mobilize immediate response to overdose spikes (ODMAP, 2018).

ODMAP functions by linking first responders, such as fire, police, and EMS, to a mapping tool that they can use on scene. It tracks overdoses and records if they are fatal or non-fatal, if

Naloxone (or Narcan) were used, the overdose location, and time/date. ODMAP is a mobile tool that is easy to use with minimal time burden.

ODMAP helps jurisdictions plan and prepare for real-time overdose spikes locally. First, a baseline for overdose spikes within a 24-hour period is established, alerts users of the app when an overdose spike is occurring in real time, allowing for local quick responses. This also supports regional and national data collection for identifying and tracking overdose trends. Use of ODMAP can also help neighboring communities mobilize swift public health responses that can reduce and prevent overdose deaths.

After a jurisdiction signs a teaming agreement, it is decided who can input data and who can view the map/data over time. Although the information on ODMAP is PHI under HIPAA, ODMAP is still HIPAA compliant and certain users covered entities under HIPAA. There are exceptions to HIPAA privacy rule that support policies and procedures of ODMAP

There are some limitations to ODMAP. Because there is no directive for jurisdictions to implement this data tool, it is used sporadically across the country and state, limiting its use for understanding where and when overdose spikes are occurring (O'Brien, 2018). It also does not use hospital/ED level data, and so there are overdoses that go missed, but it is possible this function will be added in the future.

Minnesota Opioid Dashboard

The Minnesota Opioid Dashboard is a classic dashboard that uses de-identified, aggregated state level data. The Minnesota Department of Health has developed an Opioid Dashboard, which was created "to be a one-stop shop for all statewide data related to opioid use, misuse, and overdose data prevention" (Minnesota Department of Health, 2018). This dashboard has linked healthcare related data for opioids.

Metrics include:

- Opioid overdose deaths, which are further broken down by prescriptions and heroin
    - Data source: Minnesota Death Certificates
- Nonfatal overdoses, which are broken down for ED room visits for opioids
    - Data source: Minnesota Hospital Discharge Database
- Use, misuse, and substance use disorder, which are broken down into prescription opioid misuse, heroin use, admission to treatment for opioid use disorder, and opioid treatment program percent capacity
    - Data sources:
        - National Survey on Drug Use and Health (NSDUH)
        - Minnesota Student Survey
        - Minnesota Survey of Adults Substance Use

        - Minnesota Department of Human Services: Drug and Alcohol Abuse Normative Evaluation System
- Prescribing practices, including the number of opioid prescriptions, the percent of Minnesota licensed prescribers enrolled in the prescription monitoring program, and prescribing rate among the top 500 prescribers
    - Data source: MN Prescription Monitoring Program
- Supply, Diversion, and Harm Reduction, including pharmaceuticals distributed, take-back locations, and quantity of seized drugs
    - Data sources:
        - Drug Enforcement Administration Automation of Reports and Consolidated Orders System
        - Department of Public Safety Violent Crime Enforcement Teams
- Co-occurring conditions, including hospitalization rate per diagnosis for conditions like chronic pain and opioid use disorder, opioid use hospitalizations involving suicidal ideation, infants with neonatal abstinence syndrome, and new cases of HIV with injection drug use.
    - Data source: Minnesota Hospital Discharge Database

Each metric also includes a narrative describing the metric in depth, analysis, sources used, resources and prevention strategies. This dashboard is comprehensive in its exploration of health-related opioid metrics. It displays aggregated data and does not appear to have been built on any linked individual data. However, it does not include any criminal justice data aside from drug seizures.

Cardiff Model

The Cardiff Model is a Milwaukee/West Allis based initiative for data sharing that aggregates data between hospitals, law enforcement, and EMS to target and prevent violence. This is a map type of data-sharing system.

The Cardiff Model originated in Cardiff, Wales with a physician who recognized a gap between his work in the emergency department treating victims of violence and reports of these incidents to law enforcement. He devised a model to collect data and collaborate with law enforcement and the community to predict and prevent violence. Researchers at the Medical College of Wisconsin are working on implementing a similar system in their community. Initially, their system began similarly to the model in Cardiff, Wales by tracking locations of fights and assaults when victims arrived in the ED. Eventually, they were able to add in layers of data from law enforcement and EMS to create maps about the locations of violence in their community. Recently, they received a grant which will allow them to add in information about the opioid crisis, such as opioid overdoses and PDMP data, to their existing maps.

The Cardiff Model is an aggregated data system, meaning that all the agencies extract de-identified information as an excel spreadsheet and send the data monthly to a data analyst. The data analyst then uses ArcGIS to compile the data and generate maps based on the locations of the incidents. Their system avoids double counting specific cases by applying spatial-temporal filters. If two cases were within 500 feet and 20 minutes of each other they are considered to be the same incident. Their coalition meets about once per month to view the maps and identify "hot-spots" for violence. The data is then used for prevention planning to ultimately reduce violence and opioid use in their community.

They discussed the importance of taking the time to build a strong coalition to gain the trust of the community. When they were adding new metrics to the EMR, nurse and physician champions, who held leadership positions, were vital to improving the understanding of the system changes in the ED. It was critical to change the culture in the ED from improving individual health to understanding their role in improving population health. They experienced similar encounters with law enforcement and EMS, but noted the importance of politics in collaborating with these agencies. Specifically, they mentioned that after a change in leadership, one law enforcement agency decided they did not want to contribute anymore.

The Cardiff Model was able to break down some of the specific costs associated with developing their data-sharing system. They have received a total of three grants from the Bureau of Justice and the DOJ since 2015. Initially, they had technical costs such as updating the EMR to include the necessary information. They mentioned that some hospitals were able to begin collecting data immediately, while others took years to begin data collection. Maintenance costs included the research assistant who extracts information from the EMR that costs about $4,000 per year and the data analyst who works part time developing the maps. EMS and law enforcement also charge a small fee to extract their information. The ArcGIS software costs $2,000 per year, but they mentioned that they receive a discount for being an academic institution.

They also discussed the importance of addressing legal barriers by developing data-sharing agreements between the partners. They turned to each agency to determine the type of agreement necessary to allow them to share the data, as each agency usually has a different process for data sharing. Law enforcement asked them to complete a data application, while a more formal agreement was created with the Milwaukee police department. These agencies already had a process for extracting and de-identifying information so there was less difficulty obtaining this data. The research team already had an agreement in place with the local hospitals that had IRB approval and was bound by HIPAA so it was relatively easy to obtain access to this information as well. Additionally, they discussed the importance of data stewardship, requiring each member of the coalition to sign a confidentiality agreement. Currently, their data is not available to the public because it is possible to zoom in to the street level and possibly identify individual cases.

The Camden Coalition

The Camden Coalition was founded in 2002 by a family physician who developed an electronic database from medical billing records from the three main hospitals in Camden, NJ to target super utilizers of the healthcare system. The coalition expanded to create one of the first health information exchanges (HIE) that allowed for linking of patient data across systems for improved healthcare delivery. Camden Coalition collaborators include hospitals, laboratory and radiology groups, correctional facilities, and social services organizations.

They discussed the importance of addressing organizational barriers prior to developing the data-sharing system. The organization in charge of the data needs to be trusted in the community, such as the health department. Additionally, they mentioned that looking into the community to see what information is already being collected can be beneficial because often data sharing is already happening at some level.

The Camden Coalition stressed the importance of hiring assistance in developing a data-sharing system. In creating their system, they hired an IT professional, an administrative assistant, and a data analyst. Additionally, they recommend hiring professionals who have previously worked on developing a similar system.

The startup funding for their HIE came mostly through grants to the Camden Coalition. However, most of their maintenance funding comes through partner buy-in. This means that each agency is required to pay a certain amount to become a member of the Camden Coalition and have access to the HIE.

State of Massachusetts

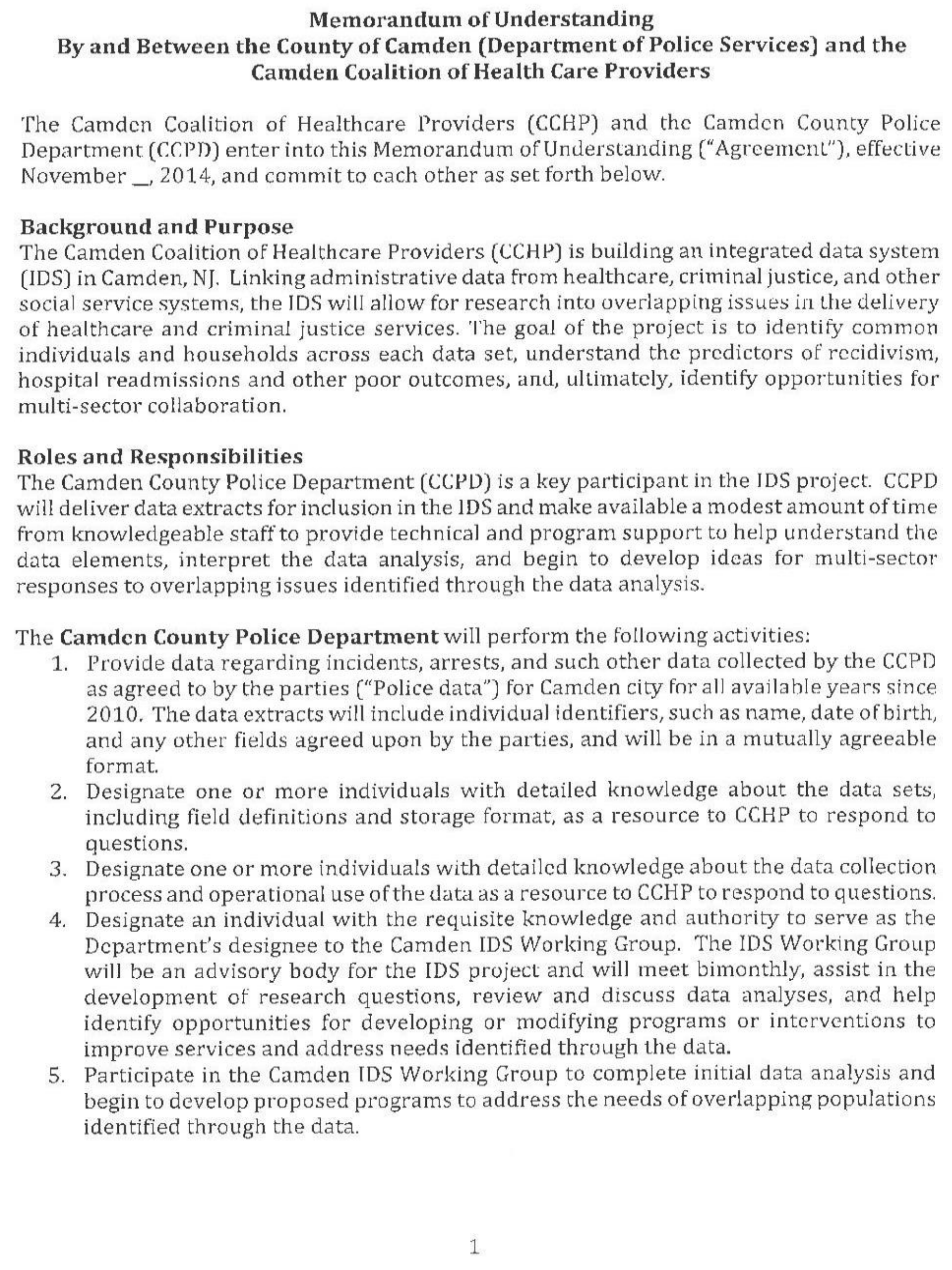
The state of Massachusetts has been hard-hit by the growing opioid epidemic. In response to this public health issue, the state allowed for sharing of data between government agencies to guide policy decisions to better address the opioid epidemic (Massachusetts Department of Public Health, 2016). The partnership took a deep dive into data surrounding opioid related issues, which allowed them to collaborate to answer critical public health question, listed in the Chapter 55 Report.

Questions they investigated include whether having multiple prescribers of opioids increases a patient’s risk of fatal opioid-related overdose, and if addition of prescription benzodiazepine to opioids increase the risk of fatal opioid-related overdose. Answering these questions has policy implications not only in Massachusetts, but the entire country.

Appendix B: Examples of Data-Sharing Agreements

The following section provides examples of data-sharing agreements or memoranda of understanding that were used in the development of existing data-sharing systems. They include memoranda of understanding between the Camden Coalition and the Department of Police Services, a HIPAA agreement between the Camden Coalition and business partners, a data-sharing agreement between the Camden Coalition and private practices, and two sample data-sharing agreements.

Memoranda of Understanding: Camden Coalition and Department of Police Services



Memorandum of Understanding
By and Between the County of Camden (Department of Police Services) and the Camden Coalition of Health Care Providers

The Camden Coalition of Healthcare Providers (CCHP) and the Camden County Police Department (CCPD) enter into this Memorandum of Understanding ("Agreement"), effective November __, 2014, and commit to each other as set forth below.

Background and Purpose

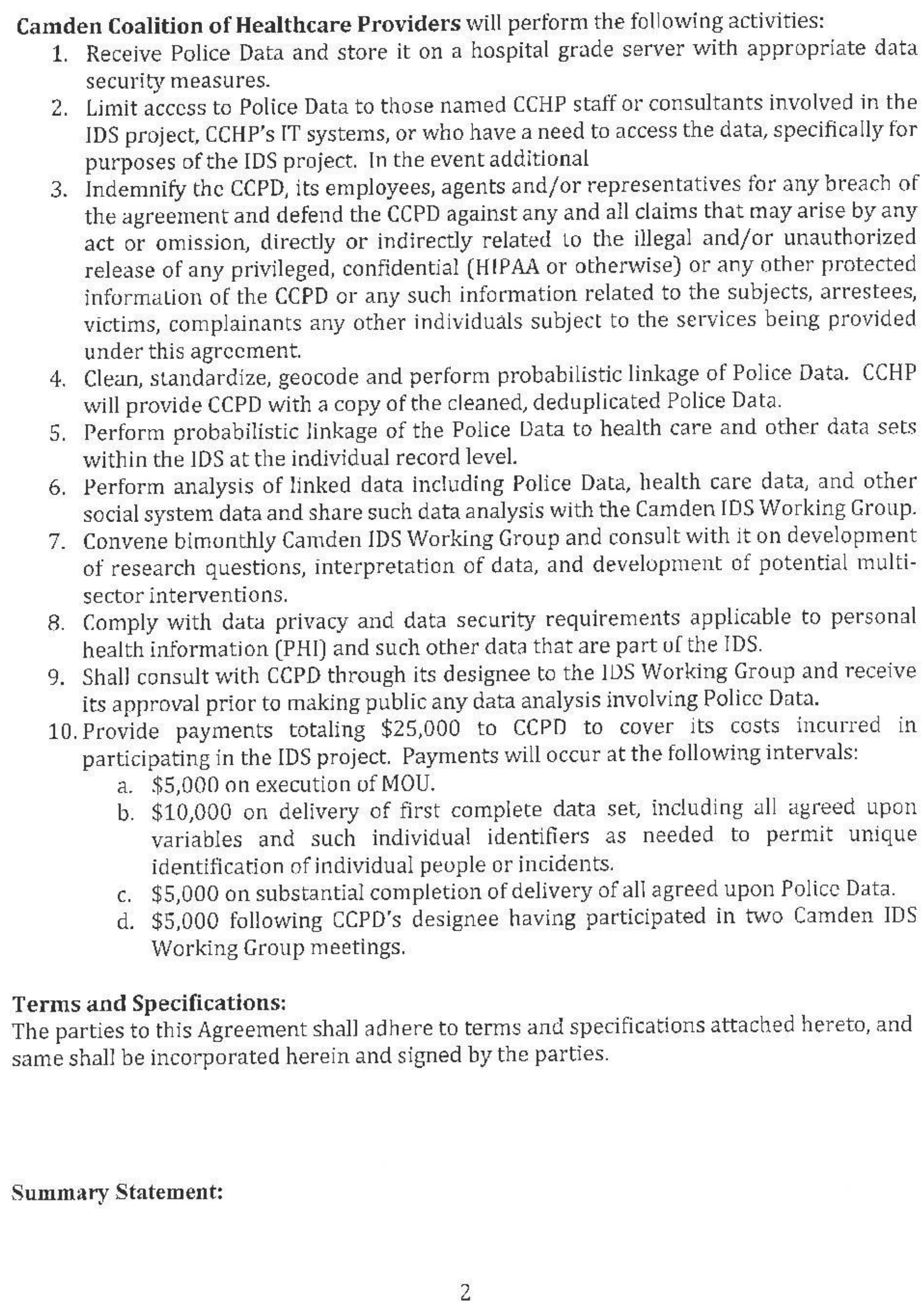
The Camden Coalition of Healthcare Providers (CCHP) is building an integrated data system (IDS) in Camden, NJ. Linking administrative data from healthcare, criminal justice, and other social service systems, the IDS will allow for research into overlapping issues in the delivery of healthcare and criminal justice services. The goal of the project is to identify common individuals and households across each data set, understand the predictors of recidivism, hospital readmissions and other poor outcomes, and, ultimately, identify opportunities for multi-sector collaboration.

Roles and Responsibilities

The Camden County Police Department (CCPD) is a key participant in the IDS project. CCPD will deliver data extracts for inclusion in the IDS and make available a modest amount of time from knowledgeable staff to provide technical and program support to help understand the data elements, interpret the data analysis, and begin to develop ideas for multi-sector responses to overlapping issues identified through the data analysis.

The **Camden County Police Department** will perform the following activities:

1. Provide data regarding incidents, arrests, and such other data collected by the CCPD as agreed to by the parties ("Police data") for Camden city for all available years since 2010. The data extracts will include individual identifiers, such as name, date of birth, and any other fields agreed upon by the parties, and will be in a mutually agreeable format.
2. Designate one or more individuals with detailed knowledge about the data sets, including field definitions and storage format, as a resource to CCHP to respond to questions.
3. Designate one or more individuals with detailed knowledge about the data collection process and operational use of the data as a resource to CCHP to respond to questions.
4. Designate an individual with the requisite knowledge and authority to serve as the Department's designee to the Camden IDS Working Group. The IDS Working Group will be an advisory body for the IDS project and will meet bimonthly, assist in the development of research questions, review and discuss data analyses, and help identify opportunities for developing or modifying programs or interventions to improve services and address needs identified through the data.
5. Participate in the Camden IDS Working Group to complete initial data analysis and begin to develop proposed programs to address the needs of overlapping populations identified through the data.



Camden Coalition of Healthcare Providers will perform the following activities:

1. Receive Police Data and store it on a hospital grade server with appropriate data security measures.
2. Limit access to Police Data to those named CCHP staff or consultants involved in the IDS project, CCHP's IT systems, or who have a need to access the data, specifically for purposes of the IDS project. In the event additional
3. Indemnify the CCPD, its employees, agents and/or representatives for any breach of the agreement and defend the CCPD against any and all claims that may arise by any act or omission, directly or indirectly related to the illegal and/or unauthorized release of any privileged, confidential (HIPAA or otherwise) or any other protected information of the CCPD or any such information related to the subjects, arrestees, victims, complainants any other individuals subject to the services being provided under this agreement.
4. Clean, standardize, geocode and perform probabilistic linkage of Police Data. CCHP will provide CCPD with a copy of the cleaned, deduplicated Police Data.
5. Perform probabilistic linkage of the Police Data to health care and other data sets within the IDS at the individual record level.
6. Perform analysis of linked data including Police Data, health care data, and other social system data and share such data analysis with the Camden IDS Working Group.
7. Convene bimonthly Camden IDS Working Group and consult with it on development of research questions, interpretation of data, and development of potential multi-sector interventions.
8. Comply with data privacy and data security requirements applicable to personal health information (PHI) and such other data that are part of the IDS.
9. Shall consult with CCPD through its designee to the IDS Working Group and receive its approval prior to making public any data analysis involving Police Data.
10. Provide payments totaling $25,000 to CCPD to cover its costs incurred in participating in the IDS project. Payments will occur at the following intervals:
    a. $5,000 on execution of MOU.
    b. $10,000 on delivery of first complete data set, including all agreed upon variables and such individual identifiers as needed to permit unique identification of individual people or incidents.
    c. $5,000 on substantial completion of delivery of all agreed upon Police Data.
    d. $5,000 following CCPD's designee having participated in two Camden IDS Working Group meetings.

Terms and Specifications:

The parties to this Agreement shall adhere to terms and specifications attached hereto, and same shall be incorporated herein and signed by the parties.

Summary Statement:

We make these commitments to one another for the purpose of developing the Camden Integrated Data System in order to better understand the relationship between health care utilization, criminal justice involvement, and other social service systems. This Agreement will be effective through November 30, 2015 unless an extension is agreed upon by both parties at an earlier date. Either party may terminate this Agreement at any time, but each party is required to give thirty (30) days written notice prior to terminating this Agreement.

Signatures of Authorized Representatives:

COUNTY OF CAMDEN
Department of Police Services

Witness:

Ross G. Angilella,
County Administrator

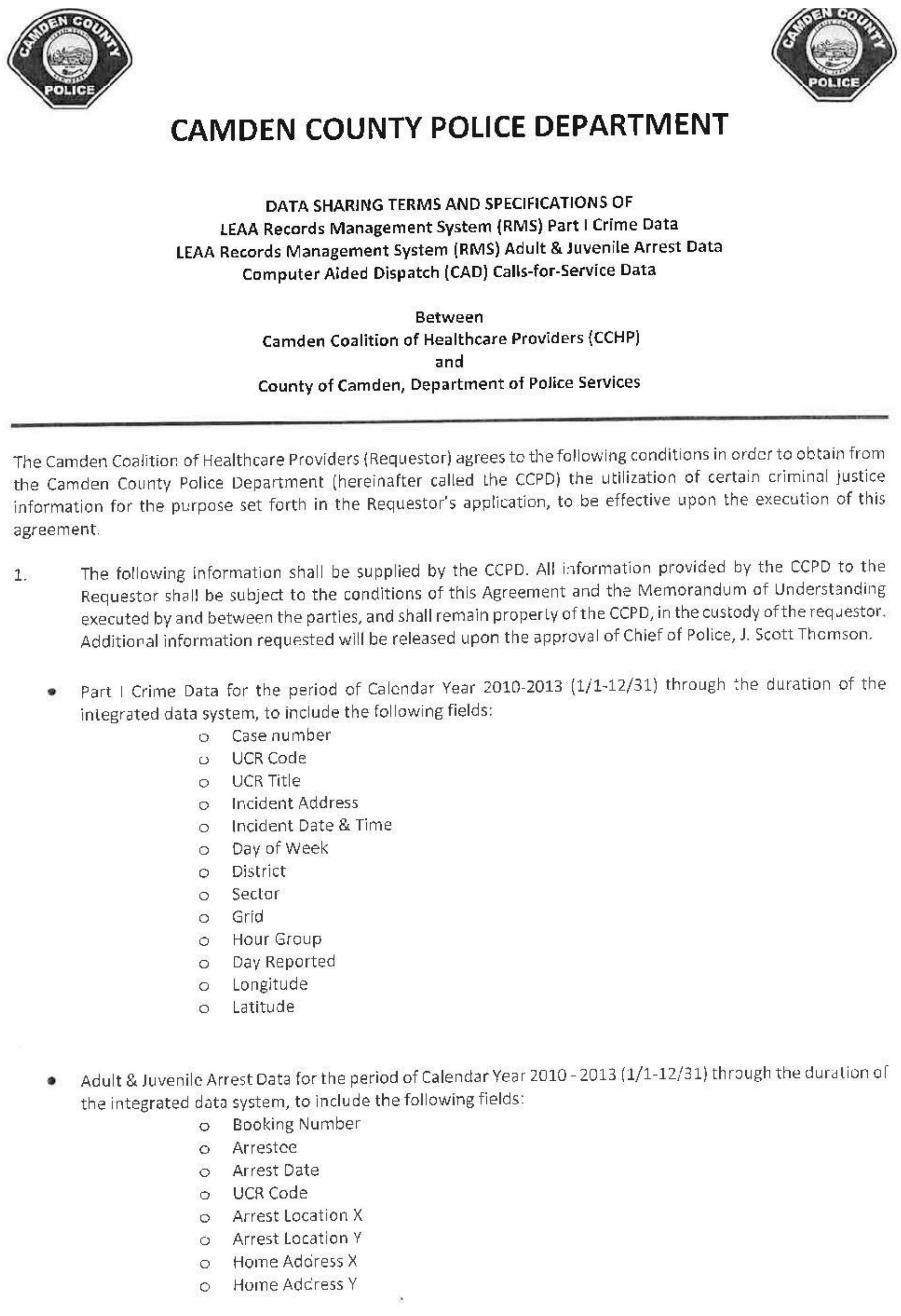
Dated:

CAMDEN COALITION OF

Witness:

Jeffrey Brenner
Executive Director

Dated:



CAMDEN COUNTY POLICE DEPARTMENT

DATA SHARING TERMS AND SPECIFICATIONS OF
LEAA Records Management System (RMS) Part I Crime Data
LEAA Records Management System (RMS) Adult & Juvenile Arrest Data
Computer Aided Dispatch (CAD) Calls-for-Service Data

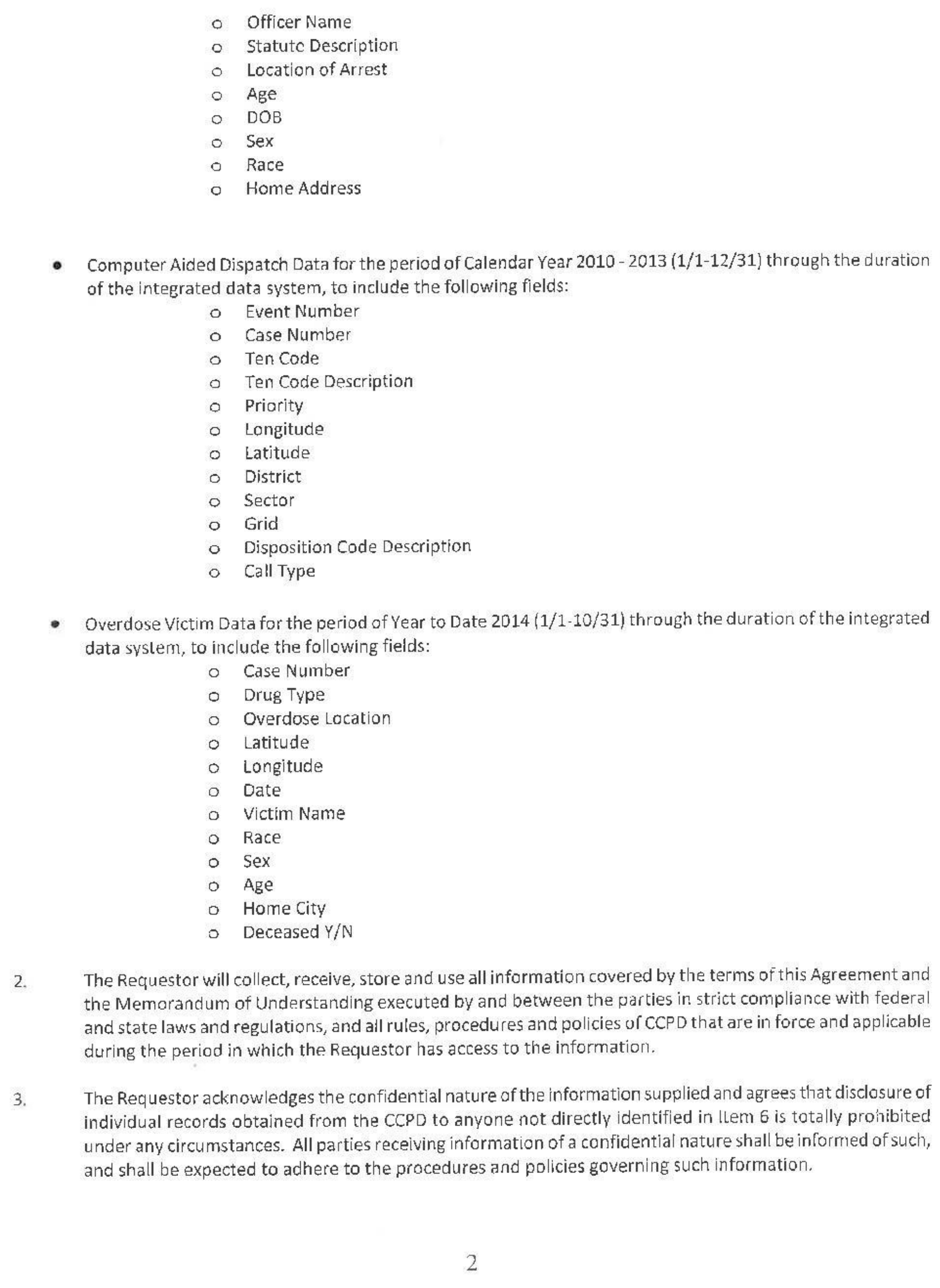
Between
Camden Coalition of Healthcare Providers (CCHP)
and
County of Camden, Department of Police Services

The Camden Coalition of Healthcare Providers (Requestor) agrees to the following conditions in order to obtain from the Camden County Police Department (hereinafter called the CCPD) the utilization of certain criminal justice information for the purpose set forth in the Requestor's application, to be effective upon the execution of this agreement.

1. The following information shall be supplied by the CCPD. All information provided by the CCPD to the Requestor shall be subject to the conditions of this Agreement and the Memorandum of Understanding executed by and between the parties, and shall remain property of the CCPD, in the custody of the requestor. Additional information requested will be released upon the approval of Chief of Police, J. Scott Thomson.

- Part I Crime Data for the period of Calendar Year 2010-2013 (1/1-12/31) through the duration of the integrated data system, to include the following fields:
  - Case number
  - UCR Code
  - UCR Title
  - Incident Address
  - Incident Date & Time
  - Day of Week
  - District
  - Sector
  - Grid
  - Hour Group
  - Day Reported
  - Longitude
  - Latitude

- Adult & Juvenile Arrest Data for the period of Calendar Year 2010 - 2013 (1/1-12/31) through the duration of the integrated data system, to include the following fields:
  - Booking Number
  - Arrestee
  - Arrest Date
  - UCR Code
  - Arrest Location X
  - Arrest Location Y
  - Home Address X
  - Home Address Y



- Officer Name
- Statute Description
- Location of Arrest
- Age
- DOB
- Sex
- Race
- Home Address

- Computer Aided Dispatch Data for the period of Calendar Year 2010 - 2013 (1/1-12/31) through the duration of the integrated data system, to include the following fields:
  - Event Number
  - Case Number
  - Ten Code
  - Ten Code Description
  - Priority
  - Longitude
  - Latitude
  - District
  - Sector
  - Grid
  - Disposition Code Description
  - Call Type

- Overdose Victim Data for the period of Year to Date 2014 (1/1-10/31) through the duration of the integrated data system, to include the following fields:
  - Case Number
  - Drug Type
  - Overdose Location
  - Latitude
  - Longitude
  - Date
  - Victim Name
  - Race
  - Sex
  - Age
  - Home City
  - Deceased Y/N

2. The Requestor will collect, receive, store and use all information covered by the terms of this Agreement and the Memorandum of Understanding executed by and between the parties in strict compliance with federal and state laws and regulations, and all rules, procedures and policies of CCPD that are in force and applicable during the period in which the Requestor has access to the information.

3. The Requestor acknowledges the confidential nature of the information supplied and agrees that disclosure of individual records obtained from the CCPD to anyone not directly identified in Item 6 is totally prohibited under any circumstances. All parties receiving information of a confidential nature shall be informed of such, and shall be expected to adhere to the procedures and policies governing such information.

4. The CCPD will determine whether all copies of the information disseminated under this request will be returned or destroyed once the use described in the application has been completed.

5. Upon completion of the project referenced in the application, the Requestor shall certify in writing that all copies of the information provided under this request have been destroyed or returned as required by Item 4 above.

6. Personnel assigned by the Requestor who will have access to the information requested are: **Aaron Truchil, Dawn Wiest, Stephen Singer, and Jean Behrand.** Additional Requestor personnel may also be given access to requested information upon mutual written agreement between the parties.

7. The Requestor has assigned himself/herself as the official custodian who shall be responsible for the maintenance, care and security of all information supplied under this Agreement.

8. If the CCPD determines that the requirements of this Agreement are not satisfactorily being met, it may require the immediate return or destruction of all copies of the information obtained under this Agreement, take such actions as it deems appropriate to protect the security and privacy of this information and enforce the terms of this contract, and refuse any future requests for criminal information from the Requestor.

9. The Requestor agrees to insert in the preface of any report citing data analysis conducted pursuant to this Agreement, whether published or unpublished, the below disclaimer by CCPD of the analysis as well as the conclusions derived:

Part I Crime Data
***Source for Part I crime data**: LEAA Records Management System (RMS) data. LEAA RMS Part I Crime Data is preliminary data to support operations that is subject to change based on a variety of reasons (i.e. late reporting, changes in classification etc). Any attempts to compare data to crime data classified under Uniform Crime Reporting (UCR) standards is strictly prohibited; therefore LEAA RMS Part I Crime Data should not be used for reporting purposes.*

Adult & Juvenile Arrest Data
***Source for arrest data**: LEAA Records Management System (RMS) data. Adult arrest data is based on data obtained from Central Booking. One person may be booked on more than one arrest charge.*

Computer Aided Dispatch Data
***Source for calls-for-service data**: LEAA Computer Aided Dispatch (CAD) calls-for-service data.*

Overdose Data
***Source for overdose data**: LEAA Records Management System (RMS) data.*

10. Requestor agrees to submit any analytical reports based on the data provided under this agreement to CCPD for review and comment prior to publication or release. CCPD shall review and comment within ten (10) days of receipt of any analytical report. Kerry Yerico, or such other person identified by the CCPD, shall be the point of contact for pre-publication review requests and comments.

11. Requestor may create and share aggregate data analysis that incorporates CCPD data with CCHP staff and others involved in the Camden IDS project, provided that each individual receiving such data signs a non-disclosure agreement. Requestor shall mark any such document Confidential: Not For Distribution, until such time that the document is submitted for CCPD review in accordance with paragraph 10. The non-disclosure agreement must be substantially similar to the one attached as Exhibit A.

12. This Agreement will become effective on the date this document is signed by both parties.

IN WITNESS WHEREOF the parties hereto have caused this agreement to be executed by their duly authorized representatives:

Camden County Police Department

By: ____________________________

Ross G. Angilella
County Administrator
County of Camden

Date: ____________________________

By: ____________________________

Kerry Yerico
Director
Criminal Intelligence & Analysis

Date: ____________________________

Requestor(s)

By: ____________________________

Jeffrey C. Brenner
Executive Director
Camden Coalition of Healthcare Providers

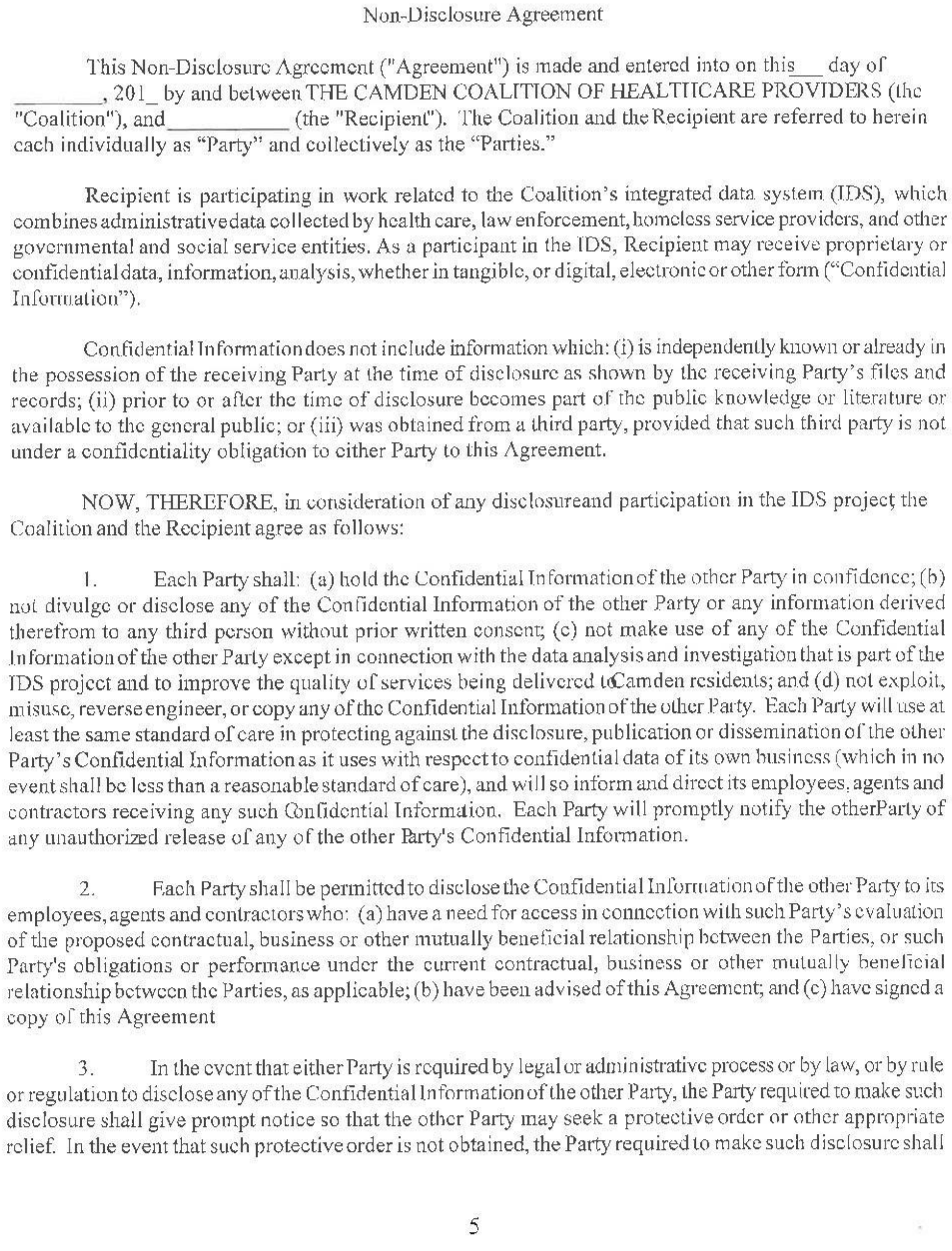
Date: ____________________________

By: ____________________________

Aaron Truchil
Associate Director of Research, Data and Evaluation
Camden Coalition of Healthcare Providers

Date: ____________________________

Exhibit A: Non-Disclosure Agreement



Non-Disclosure Agreement

This Non-Disclosure Agreement ("Agreement") is made and entered into on this___ day of ________, 201_ by and between THE CAMDEN COALITION OF HEALTHCARE PROVIDERS (the "Coalition"), and___________ (the "Recipient"). The Coalition and the Recipient are referred to herein each individually as "Party" and collectively as the "Parties."

Recipient is participating in work related to the Coalition's integrated data system (IDS), which combines administrative data collected by health care, law enforcement, homeless service providers, and other governmental and social service entities. As a participant in the IDS, Recipient may receive proprietary or confidential data, information, analysis, whether in tangible, or digital, electronic or other form ("Confidential Information").

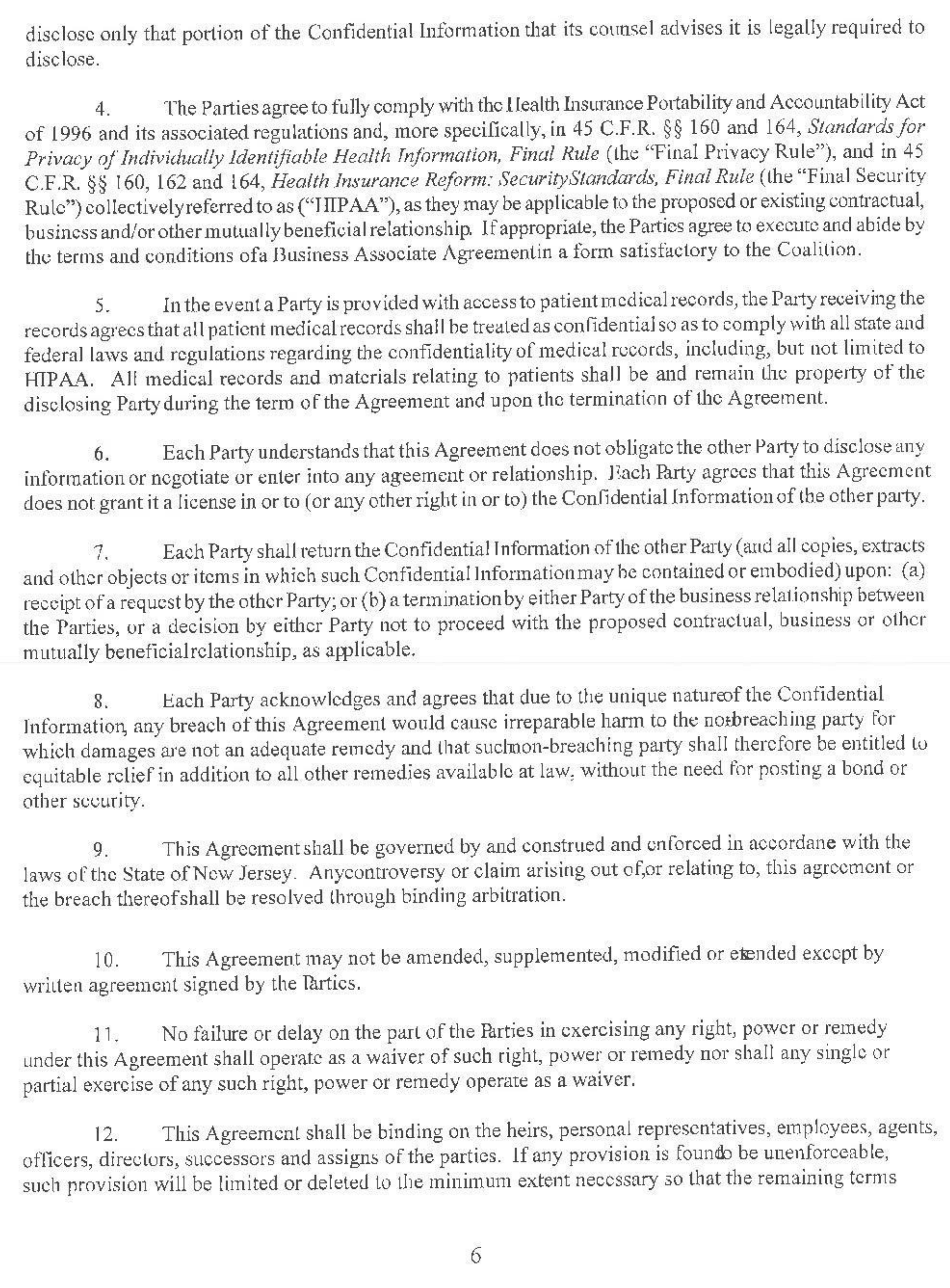
Confidential Information does not include information which: (i) is independently known or already in the possession of the receiving Party at the time of disclosure as shown by the receiving Party's files and records; (ii) prior to or after the time of disclosure becomes part of the public knowledge or literature or available to the general public; or (iii) was obtained from a third party, provided that such third party is not under a confidentiality obligation to either Party to this Agreement.

NOW, THEREFORE, in consideration of any disclosureand participation in the IDS project, the Coalition and the Recipient agree as follows:

1. Each Party shall: (a) hold the Confidential Information of the other Party in confidence; (b) not divulge or disclose any of the Confidential Information of the other Party or any information derived therefrom to any third person without prior written consent; (c) not make use of any of the Confidential Information of the other Party except in connection with the data analysis and investigation that is part of the IDS project and to improve the quality of services being delivered toCamden residents; and (d) not exploit, misuse, reverse engineer, or copy any of the Confidential Information of the other Party. Each Party will use at least the same standard of care in protecting against the disclosure, publication or dissemination of the other Party's Confidential Information as it uses with respect to confidential data of its own business (which in no event shall be less than a reasonable standard of care), and will so inform and direct its employees, agents and contractors receiving any such Confidential Information. Each Party will promptly notify the otherParty of any unauthorized release of any of the other Party's Confidential Information.

2. Each Party shall be permitted to disclose the Confidential Information of the other Party to its employees, agents and contractors who: (a) have a need for access in connection with such Party's evaluation of the proposed contractual, business or other mutually beneficial relationship between the Parties, or such Party's obligations or performance under the current contractual, business or other mutually beneficial relationship between the Parties, as applicable; (b) have been advised of this Agreement; and (c) have signed a copy of this Agreement

3. In the event that either Party is required by legal or administrative process or by law, or by rule or regulation to disclose any of the Confidential Information of the other Party, the Party required to make such disclosure shall give prompt notice so that the other Party may seek a protective order or other appropriate relief. In the event that such protective order is not obtained, the Party required to make such disclosure shall



disclose only that portion of the Confidential Information that its counsel advises it is legally required to disclose.

4. The Parties agree to fully comply with the Health Insurance Portability and Accountability Act of 1996 and its associated regulations and, more specifically, in 45 C.F.R. §§ 160 and 164, *Standards for Privacy of Individually Identifiable Health Information, Final Rule* (the "Final Privacy Rule"), and in 45 C.F.R. §§ 160, 162 and 164, *Health Insurance Reform: SecurityStandards, Final Rule* (the "Final Security Rule") collectivelyreferred to as ("HIPAA"), as they may be applicable to the proposed or existing contractual, business and/or other mutually beneficial relationship. If appropriate, the Parties agree to execute and abide by the terms and conditions ofa Business Associate Agreementin a form satisfactory to the Coalition.

5. In the event a Party is provided with access to patient medical records, the Party receiving the records agrees that all patient medical records shall be treated as confidential so as to comply with all state and federal laws and regulations regarding the confidentiality of medical records, including, but not limited to HIPAA. All medical records and materials relating to patients shall be and remain the property of the disclosing Partyduring the term of the Agreement and upon the termination of the Agreement.

6. Each Party understands that this Agreement does not obligate the other Party to disclose any information or negotiate or enter into any ageement or relationship. Each Party agrees that this Agreement does not grant it a license in or to (or any other right in or to) the Confidential Information of the other party.

7. Each Party shall return the Confidential Information of the other Party (and all copies, extracts and other objects or items in which such Confidential Informationmay be contained or embodied) upon: (a) receipt of a request by the other Party; or (b) a terminationby either Party of the business relationship between the Parties, or a decision by either Party not to proceed with the proposed contractual, business or other mutually beneficialrelationship, as applicable.

8. Each Party acknowledges and agrees that due to the unique natureof the Confidential Information, any breach of this Agreement would cause irreparable harm to the non-breaching party for which damages are not an adequate remedy and that suchnon-breaching party shall therefore be entitled to equitable relief in addition to all other remedies available at law, without the need for posting a bond or other security.

9. This Agreement shall be governed by and construed and enforced in accordane with the laws of the State of New Jersey. Anycontroversy or claim arising out of,or relating to, this agreement or the breach thereofshall be resolved through binding arbitration.

10. This Agreement may not be amended, supplemented, modified or extended except by written agreement signed by the Parties.

11. No failure or delay on the part of the Parties in exercising any right, power or remedy under this Agreement shall operate as a waiver of such right, power or remedy nor shall any single or partial exercise of any such right, power or remedy operate as a waiver.

12. This Agreement shall be binding on the heirs, personal representatives, employees, agents, officers, directors, successors and assigns of the parties. If any provision is foundto be unenforceable, such provision will be limited or deleted to the minimum extent necessary so that the remaining terms

remain in full force and effect.

13. The term of this Agreement is 36 months from the effective date of the Agreement unless before the end of the term either Party terminatesthe business relationship between the Parties, or either Party decides not to proceed with the proposedcontractual, business or other mutually beneficial relationship pursuant to Section 7 of this Agreement.

IN WITNESS WHEREOF the parties hereto have caused this agreement to be executed by their duly authorized representatives.

CAMDEN COALITION OF HEALTHCARE PROVIDERS

By:______________________

Name:______________________

Title:______________________

Date:______________________

RECIPIENT

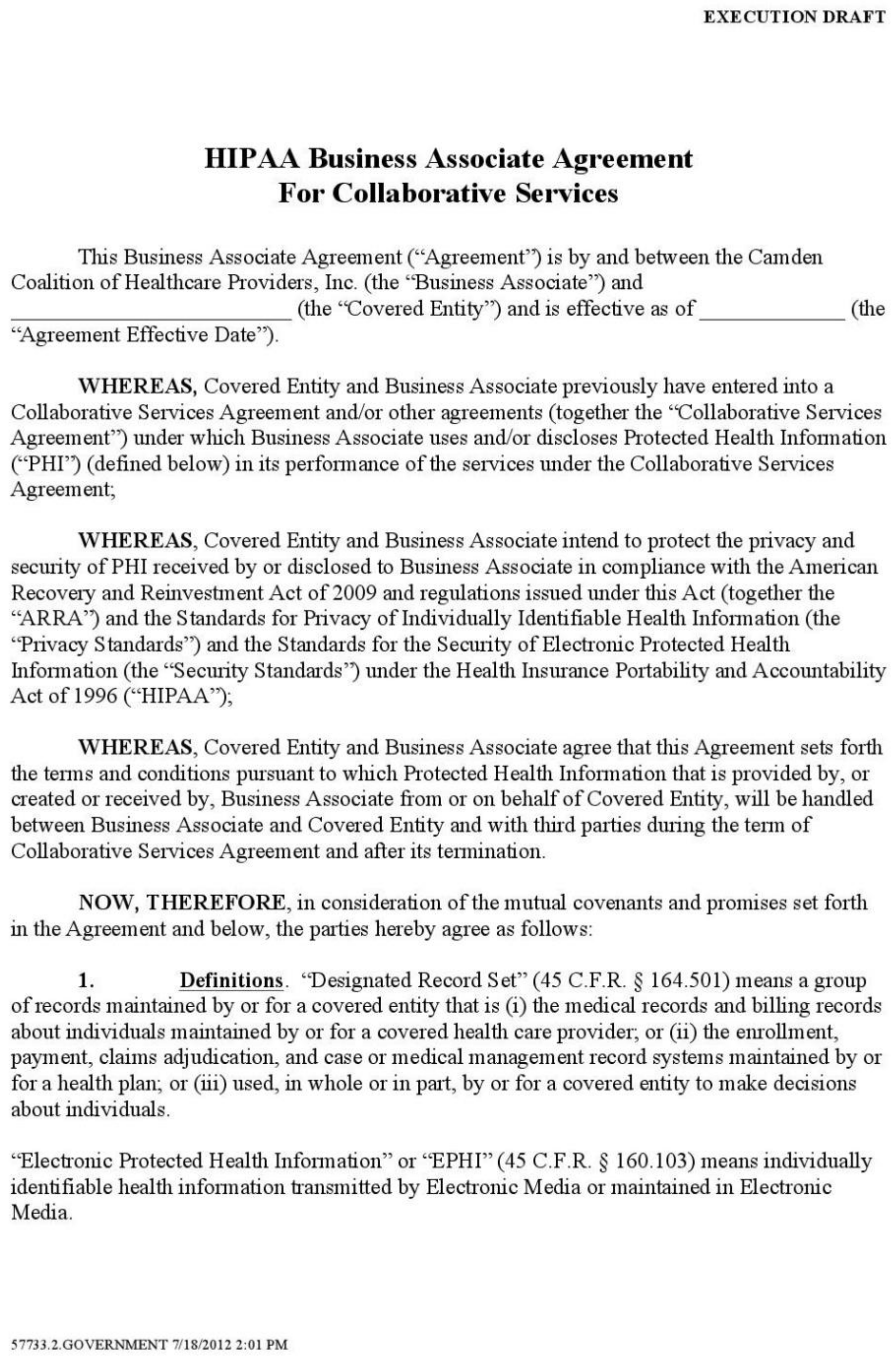
By:______________________

Organization:________________

Title:______________________

Date:______________________

HIPAA Agreement: Camden Coalition and Business Associates



EXECUTION DRAFT

HIPAA Business Associate Agreement
For Collaborative Services

This Business Associate Agreement ("Agreement") is by and between the Camden Coalition of Healthcare Providers, Inc. (the "Business Associate") and _________________________ (the "Covered Entity") and is effective as of _____________ (the "Agreement Effective Date").

WHEREAS, Covered Entity and Business Associate previously have entered into a Collaborative Services Agreement and/or other agreements (together the "Collaborative Services Agreement") under which Business Associate uses and/or discloses Protected Health Information ("PHI") (defined below) in its performance of the services under the Collaborative Services Agreement;

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and security of PHI received by or disclosed to Business Associate in compliance with the American Recovery and Reinvestment Act of 2009 and regulations issued under this Act (together the "ARRA") and the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Standards") and the Standards for the Security of Electronic Protected Health Information (the "Security Standards") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA");

WHEREAS, Covered Entity and Business Associate agree that this Agreement sets forth the terms and conditions pursuant to which Protected Health Information that is provided by, or created or received by, Business Associate from or on behalf of Covered Entity, will be handled between Business Associate and Covered Entity and with third parties during the term of Collaborative Services Agreement and after its termination.

NOW, THEREFORE, in consideration of the mutual covenants and promises set forth in the Agreement and below, the parties hereby agree as follows:

1. **Definitions**. "Designated Record Set" (45 C.F.R. § 164.501) means a group of records maintained by or for a covered entity that is (i) the medical records and billing records about individuals maintained by or for a covered health care provider; or (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for a covered entity to make decisions about individuals.

"Electronic Protected Health Information" or "EPHI" (45 C.F.R. § 160.103) means individually identifiable health information transmitted by Electronic Media or maintained in Electronic Media.

57733.2.GOVERNMENT 7/18/2012 2:01 PM

"Electronic Media" (45 C.F.R. § 160.103) means (1) electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as a magnetic tape or disk, optical disk, or digital memory card; or (2) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.

"Individual" (45 C.F.R. § 160.103) means the person who is the subject of Protected Health Information.

"Individually Identifiable Health Information" (45 C.F.R. § 160.103) means information, including demographic information, collected from an individual and (i) is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and (ii) relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual; and (a) identifies the individual, or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Protected Health Information" ("PHI") (45 C.F.R. § 160.103) means Individually Identifiable Health Information that is (i) transmitted by electronic media; (ii) maintained in any medium constituting electronic media; or (iii) transmitted or maintained in any other form or medium.

"Security Breach" (as defined under the ARRA, including certain exceptions) means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information.

"Security Incident" (45 C.F.R. § 164.304) means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

2. **Use and Disclosure of PHI**. Business Associate may receive PHI from multiple sources, including but not limited to: (a) Covered Entity pursuant to the Collaborative Services Agreement; (b) other covered entities pursuant to Covered Entity's collaborative services agreements with such other covered entities; and (c) other Camden Health Information Exchange ("HIE") participants through Business Associate's participation in the HIE. Business Associate may use and disclose HIE data and any PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity only as permitted or required by the Collaborative Services Agreement, this Agreement or as otherwise permitted or required by law. The services provided by Business Associate under the Collaborative Services Agreement include care management, certain consulting services, and HIE coordination. All such uses and disclosures also shall be in compliance with each applicable requirement of 45 C.F.R. § 164.504(e). Business Associate shall not, and shall ensure that its directors, officers, employees, contractors, and agents do not use or disclose PHI received from Covered Entity or

6 **Mitigation**. Business Associate agrees 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 in violation of the requirements of this Agreement.

7. **Reporting of Disclosures of PHI**. Business Associate shall report to Covered Entity within forty-eight (48) hours any Security Incident, Security Breach or use or disclosure of PHI in violation of this Agreement of which it becomes aware. A Security Breach/Incident will be considered "discovered" by Noteworthy as of the first day on which such Breach/Incident is known to Business Associate (including any person, other than the individual committing the Breach/Incident, that is an employee, officer, or other agent of Business Associate), or should reasonably have been known to Business Associate to have occurred. Business Associate's initial reports to Covered Entity regarding Security Breaches/Incidents shall include the identification of each Individual whose unsecured PHI (as defined under ARRA and the HIPAA Standards) has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Breach/Incident, as well as the type of PHI accessed, acquired or disclosed. Business Associate shall take prompt corrective action to cure any deficiencies and will take any action pertaining to such Security Breach/Incident required by applicable federal and state laws and regulations. Business Associate will provide a written report to Covered Entity within fifteen (15) days of the discovery of any use or disclosure of Covered Entity's PHI not permitted by this Agreement, and such report shall describe in detail: (i) the actions taken by Business Associate to mitigate any harmful effect of the unauthorized use or disclosures and (ii) what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure. To the extent Business Associate coordinates and assists Covered Entity in providing notice of the Security Breach/Incident to Individuals, Business Associate agrees to do so in accordance with the ARRA, including without limitation ARRA provisions regarding timeliness, content and recipients of such notice.

8. **Agreements with Third Parties**. Business Associate agrees to require any agent or subcontractor to whom it provides PHI to agree in writing to be bound by the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such PHI. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate safeguards to protect the EPHI. Business Associate shall disclose to such subcontractors or agents only the minimum PHI necessary (as defined under the HIPAA Standards and the ARRA) to perform or fulfill a specific function required or permitted under the Collaborative Services Agreement or this Agreement.

9. **Access to Information**. Business Associate agrees to provide access, at the request of Covered Entity or an Individual, to PHI in a Designated Record Set to the Individual or Covered Entity so that Covered Entity may meet the requirements of 45 C.F.R. § 164.524 and the ARRA (including access to the information in electronic format as required under the ARRA).

10. **Amendments/Availability of PHI for Amendment**. Business Associate agrees to make any amendments to PHI in a Designated Record Set that the Covered Entity directs in accordance with the requirements of 45 C.F.R. § 164.526.

11. **Accounting of Disclosures**. Business Associate agrees to document such disclosures of PHI and information related to such disclosures, and retain such documentation and information, as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and the ARRA. Business Associate agrees to respond to requests from Covered Entity or an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and the ARRA. As required under the ARRA, Business Associate agrees to respond to Individual requests for accountings relating to electronic health records if Covered Entity includes Business Associate on a list of business associates who may respond on Covered Entity's behalf.

12 **Restrictions**. Business Associate agrees to respond to requests by an Individual for restrictions on the use and disclosure of PHI in accordance with 45 C.F.R. § 164.522 (or implement a restriction agreed to by Covered Entity), including requests for confidential communications, and to notify Covered Entity immediately regarding any restrictions to which Business Associate agrees. Business Associate also agrees to comply with a request for a restriction if the disclosure is to a health plan for the purposes of carrying out payment or health care operations (and is not for treatment) and the PHI pertains solely to a healthcare item or services for which the health care provider involved has been paid out of pocket in full.
.

13. **Availability of Books and Records**. Business Associate hereby agrees to make its internal policies, procedures, practices, books, records and agreements relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of the Department of Health and Human Services (the "Secretary") for purposes of determining Covered Entity's compliance with the Privacy and Security Standards and the ARRA.

14. **Return of PHI upon Termination**. Upon termination of the Collaborative Services Agreement or this Agreement for any reason, Business Associate shall return all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity and which Business Associate still maintains in any form. Prior to doing so, Business Associate further agrees to recover any PHI in the possession of its subcontractors or agents. Business Associate shall not retain any copies of such PHI.

If it is not feasible to return such PHI, Business Associate agrees to extend any and all protections, limitations, and restrictions in this Agreement to the Business Associate's use and disclosure of any PHI retained after the termination of the Agreement, and to limit any further uses and disclosures to the purpose or purposes that make the return of PHI infeasible. If it is not feasible for Business Associate to obtain from a subcontractor or agent any PHI in the possession of the subcontractor or agent, Business Associate must require the subcontractor and/or agent to agree in writing to extend any and all protections, limitations, and restrictions in this Agreement to the subcontractors' and/or agents' use and disclosure of any PHI retained after the termination of the Agreement, and to limit any further uses and disclosures to the purposes that make the return of the PHI infeasible.

15. **Termination**. Covered Entity may immediately terminate the Collaborative Services Agreement and this Agreement and any related agreements if Covered Entity determines that Business Associate has breached a material term of this Agreement. Alternatively, Covered Entity may (i) provide Business Associate with thirty (30) days written notice of the existence of an alleged material breach; and (ii) afford Business Associate an opportunity to cure said alleged material breach to Covered Entity's satisfaction within the stated time period. Failure to cure the alleged breach to Covered Entity's satisfaction within such time period is grounds for immediate termination of the Agreement; provided, however, that in the event that Covered Entity determines that termination of the Agreement is not feasible, Business Associate hereby acknowledges that Covered Entity shall have the right to report the breach to the Secretary, notwithstanding any other provision of the Agreement to the contrary. To the extent that Business Associate knows of a pattern of activity or practice of Covered Entity that constitutes a material breach or violation of Covered Entity's obligations under this Agreement, Business Associate will take reasonable steps to assist Covered Entity in curing the breach or ending the violation, and if such steps are unsuccessful, Business Associate may terminate this Agreement and the Collaborative Services Agreement, if feasible. If termination is not feasible, Business Associate may report the problem to the Secretary.

16. **No Third Party Beneficiaries**. Nothing in the Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

17. **Covered Entity's Obligations.** Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

18. **Regulatory References**. A reference in the Agreement to a section in the Privacy or Security Standards and the ARRA means the section as in effect or as amended from time to time.

19. **Amendment**. No changes, amendments, or alterations of this Agreement shall be effective unless signed by duly authorized representatives of both parties, except as expressly provided herein. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the Privacy or Security Standards, the ARRA, or other applicable law.

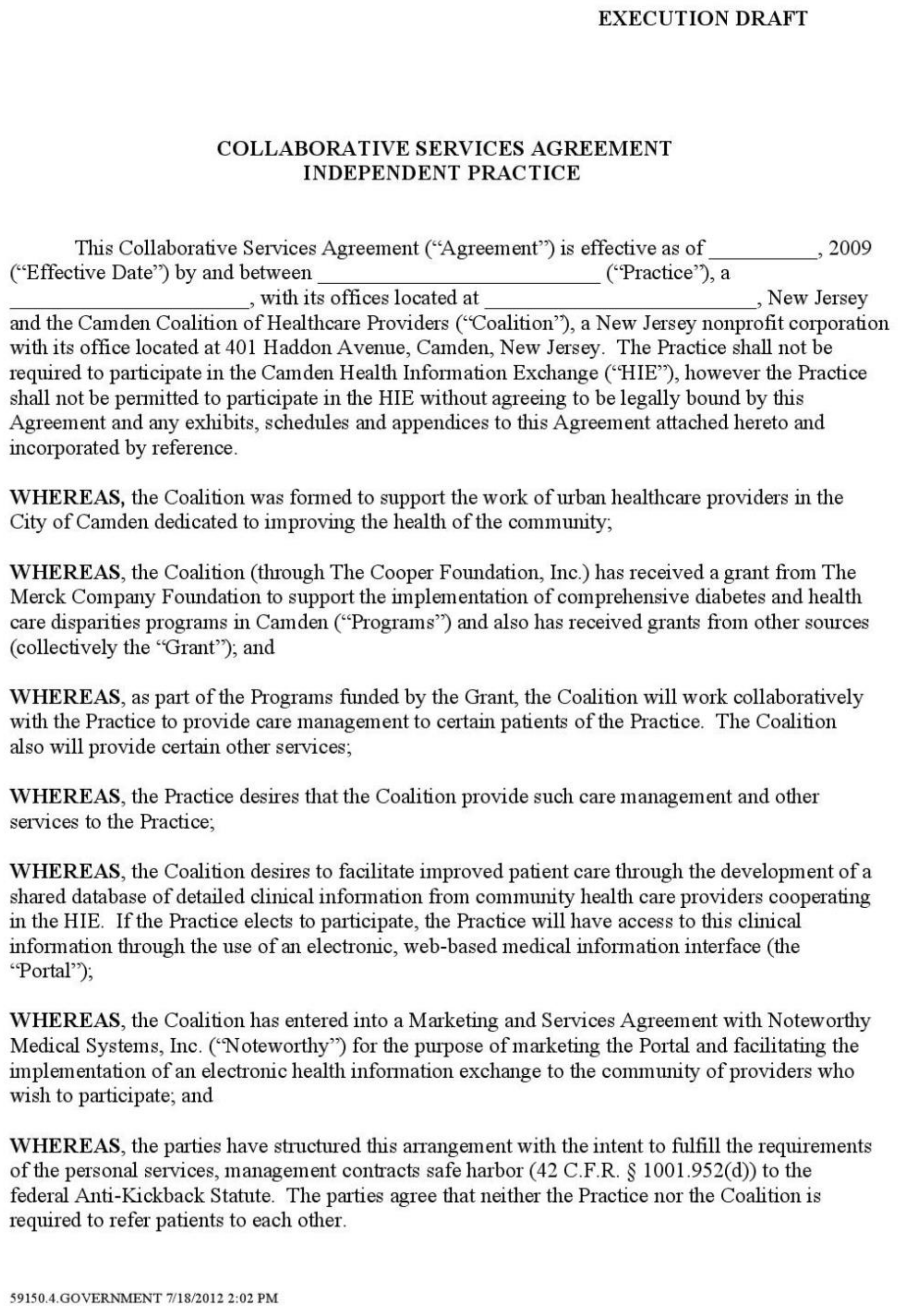
IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Agreement Effective Date.

COVERED ENTITY **BUSINESS ASSOCIATE**

By: ____________________________ ________________________________

Name: __________________________ ________________________________
Title: ___________________________ ________________________________
Date: ___________________________ ________________________________

Data Sharing Agreement: Camden Coalition and Private Practices



EXECUTION DRAFT

COLLABORATIVE SERVICES AGREEMENT
INDEPENDENT PRACTICE

This Collaborative Services Agreement ("Agreement") is effective as of __________, 2009 ("Effective Date") by and between _________________________ ("Practice"), a ______________________, with its offices located at ________________________, New Jersey and the Camden Coalition of Healthcare Providers ("Coalition"), a New Jersey nonprofit corporation with its office located at 401 Haddon Avenue, Camden, New Jersey. The Practice shall not be required to participate in the Camden Health Information Exchange ("HIE"), however the Practice shall not be permitted to participate in the HIE without agreeing to be legally bound by this Agreement and any exhibits, schedules and appendices to this Agreement attached hereto and incorporated by reference.

WHEREAS, the Coalition was formed to support the work of urban healthcare providers in the City of Camden dedicated to improving the health of the community;

WHEREAS, the Coalition (through The Cooper Foundation, Inc.) has received a grant from The Merck Company Foundation to support the implementation of comprehensive diabetes and health care disparities programs in Camden ("Programs") and also has received grants from other sources (collectively the "Grant"); and

WHEREAS, as part of the Programs funded by the Grant, the Coalition will work collaboratively with the Practice to provide care management to certain patients of the Practice. The Coalition also will provide certain other services;

WHEREAS, the Practice desires that the Coalition provide such care management and other services to the Practice;

WHEREAS, the Coalition desires to facilitate improved patient care through the development of a shared database of detailed clinical information from community health care providers cooperating in the HIE. If the Practice elects to participate, the Practice will have access to this clinical information through the use of an electronic, web-based medical information interface (the "Portal");

WHEREAS, the Coalition has entered into a Marketing and Services Agreement with Noteworthy Medical Systems, Inc. ("Noteworthy") for the purpose of marketing the Portal and facilitating the implementation of an electronic health information exchange to the community of providers who wish to participate; and

WHEREAS, the parties have structured this arrangement with the intent to fulfill the requirements of the personal services, management contracts safe harbor (42 C.F.R. § 1001.952(d)) to the federal Anti-Kickback Statute. The parties agree that neither the Practice nor the Coalition is required to refer patients to each other.

NOW THEREFORE, in consideration of the mutual promises and obligations hereinafter contained, the parties hereto intend to be legally bound and mutually agree upon the following terms and conditions:

A. SERVICES AND DUTIES:

1. The Coalition will provide care management to certain patients referred to the Coalition by the Practice. Depending on the needs of each patient, the care management services may include individualized case management, individual/group education, home visits, and coordination of specialty care. The Coalition also will provide the services targeted to the Practice described in the Exhibits attached hereto and made a part hereof. The care management and any services checked in Exhibit A are referred to herein as the "Services." **The Practice may elect to participate in the Health Information Exchange by electing such Service on Exhibit A and signing Exhibit B.**

2. The number of patients to whom the care management services will be provided is limited by the Grant and the Practice will refer to the Coalition only its most severe cases. Due to the limits of the Grant funding, the Coalition has discretion to accept or reject patients for the Programs. The Coalition shall not accept or reject patients based on their insurance status or any other discriminatory process.

3. The Coalition case managers will provide Services to patients at Practice sites, in the community, and during home visits.

4. The Coalition will communicate with the staff at Practice's site on a regular basis.

5. The Practice will provide the Coalition with access to patient medical information for the purpose of patient care, tracking, follow-up and coordination with the additional Services described in Exhibit A. The Coalition and the Practice agree to enter into a HIPAA Business Associate Agreement covering the Coalition's use and disclosure of protected health information received from or on behalf of the Practice.

B. COMPENSATION

1. All Services provided by the Coalition under this Agreement shall be reimbursed pursuant to the Grant, unless the Services provided to the patient are covered under the patient's insurance plan. The Practice shall not be responsible for payment to the Coalition for these Services. To the extent that third party payment (whether private or public) is available for services provided to patients, each party will bill applicable third party payors for the services they provide to patients.

C. INDEPENDENT CONTRACTORS

1. Nothing in this Agreement shall be construed to create a joint venture or partnership between the parties. Each party shall act solely as an independent contractor and not as an agent, servant, employee, or representative of the other party.

D. GOVERNING LAW

1. This Agreement shall be governed and interpreted according to the laws of the State of New Jersey without regard to choice of law principles.

E. COMPLIANCE WITH LAW/ABILITY TO CONTRACT

1. The parties represent and warrant that they will perform their respective obligations under this Agreement in conformity with any applicable laws, regulations, and other legal mandates. Each represents and warrants that it has the unqualified right, power, and authority to enter into this Agreement and that it does not know or have reason to believe of anything that will prevent it from performing its obligations under the terms and conditions of this Agreement.

F. QUALIFICATIONS OF STAFF PERFORMING SERVICES

1. Coalition staff providing Services under this Agreement shall have and maintain appropriate licensure/registration, as required in the state of New Jersey, and shall not be subject to any disciplinary restrictions, nor shall they have been excluded or debarred from participation in any government payor program. Such staff also shall maintain appropriate malpractice insurance as required by New Jersey law.

G. TERM/TERMINATION

1. This Agreement shall be effective for an initial term of one (1) year from its effective date and thereafter shall automatically renew for additional terms of one (1) year each, unless and until the Grant is completed or terminated.

2. This Agreement may be terminated at any time by either party upon at least thirty (30) days' prior written notice of such termination to the other party for default or material breach by the other party of one or more of its obligations hereunder, unless such default or breach is cured within thirty (30) days of the notice of termination. This Agreement may be terminated by the Coalition upon at least thirty (30) days' prior written notice due to completion or termination of the Grant.

3. This Agreement may be terminated without cause at any time by either party upon at least sixty (60) days' prior written notice of such termination to the other party.

H. NOTICES

1. Any notice or communication required or permitted by this Agreement shall be in writing and shall be deemed sufficient upon receipt, when delivered personally or by courier, overnight delivery service or confirmed facsimile, or forty-eight (48) hours after being deposited in the regular mail as certified or registered mail (airmail if sent internationally) with postage prepaid, if such notice is addressed to the party to be notified at such party's address or facsimile number as set forth below, or as subsequently modified by written notice.

If to Coalition: Jeffrey C. Brenner, M.D.
Camden Coalition of Healthcare Providers
401 Haddon Avenue
Camden, NJ 08103

If to Practice: [insert name, title, and address]

Either of the parties may, in its sole discretion, designate new person(s) or address(es) for receipt of notices by providing written notice to the other party.

I. ENTIRE AGREEMENT/ASSIGNMENT

1. This Agreement, including all exhibits and attachments, constitutes the complete and sole understanding between the Practice and the Coalition with respect to its subject matter and supersedes any and all prior or contemporaneous communications, discussions, agreements, understandings, promises, and/or representations made by either party to the other, whether oral, written, or in any other form, not expressly included herein. No changes, amendments, or alterations shall be effective unless signed by duly authorized representatives of both parties. Neither party may assign any of its rights or delegate is obligations hereunder without the prior written consent of the other parties hereto, and such consent shall not be unreasonably withheld.

J. SEVERABILITY

1. Any determination that any provision of this Agreement or any application thereof is invalid, illegal or unenforceable in any respect in any instance shall not affect the validity, legality, and enforceability of such provision in any other instance, or the validity, legality, or enforceability of any other provision of this Agreement.

K. WAIVER

1. The waiver by either party of a breach or violation of any provision of this Agreement shall not operate or be construed to be a waiver of any subsequent breach or violation thereof. To be effective, all waivers must be in writing and signed by an authorized officer of the party to be charged.

L. COUNTERPARTS

1. This Agreement may be executed in one or more counterparts, each of which will be deemed to be an original copy of this Agreement and all of which, when taken together, will be deemed to constitute one and the same agreement.

M. HEADINGS

1. The headings contained in this Agreement are included for purposes of convenience only, and shall not affect in any way the meaning or interpretation of any of the terms or provisions of this Agreement.

IN WITNESS WHEREOF, the parties, through their duly authorized officers, have executed this Agreement effective as of the Effective Date.

PRACTICE	**CAMDEN COALITION OF HEALTHCARE PROVIDERS**
By: ______________________________	______________________________
Print Name: ______________________	______________________________
Print Title: _______________________	______________________________
Date: ____________________________	______________________________

EXHIBIT A

Additional Services

The Coalition will provide the Practice with the following additional services listed below as checked and initialed by both parties.

___ Access to the Camden Health Information Exchange through an electronic medical records interface or Portal; (**If this is checked, Practice must review and sign Exhibit B.**)

___ Consulting services relating to Practice improvement;

___ Consulting services relating to implementation of Electronic Health Records;

___ Consulting services relating to developing a patient registry and identifying high cost/high needs patients through matching of practice data to hospital data;

___ Consulting services regarding implementing open access scheduling;

___ Consulting services to conduct group medical visits

___ Consulting services regarding the use of community health workers;

___ Consulting services regarding the use of the chronic care model;

___ Provider/staff training and education, including:

- ___ Specialty consultation/education/training;
- ___ Practice management education/training; and
- ___ Continuing Medical Education.

___ Consulting services relating to practice/provider certifications, including:

- ___ Practice NCQA Certification at a Patient Centered Medical Home;
- ___ Practice ADA Diabetes Education Recognition Program;
- ___ Provider NCQA Certification in Diabetes Provider Program; and

___ Patient outreach/care management to high need/high cost patients.

EXHIBIT B

HEALTH INFORMATION EXCHANGE

PARTICIPATION AGREEMENT

The parties to the Agreement above have elected to access the Camden Health Information Exchange through an electronic medical records interface or Portal and agree to be legally bound by the Participation Agreement as follows.

1. The Coalition agrees to provide the Practice with access to the Portal at no cost to the Practice contingent upon the availability of funds. As noted in Section B of the Agreement, all Services are reimbursed pursuant to the Grant.

2. The Coalition shall comply with certain participation criteria (the "HIE Participation Criteria") attached herein and incorporated by reference. For purposes of this Participation Agreement, an HIE Participant includes but is not limited to, a Practice, its Authorized Users, as defined below, the Coalition and any other person or entity which has authorized access to the Portal.

3. The Coalition, subject to appropriate patient authorization, may utilize the data it obtains as an HIE Participant to (a) create citywide, clinic-level, and provider-level patient registries for improving care of chronic illnesses, high utilizing patients, and prevention screening; (b) conduct public health research (subject to obtaining the permission of the Institutional Review Boards of affected providers, as applicable); (c) provide care management of complex patients who frequently use emergency rooms and hospitals, including through the establishment of real-time alerts for patients currently being managed, and notification regarding new patients that exceed pre-set utilization criteria; and (d) enable the Coalition's care management team to review labs, radiology, and discharge summaries of patients currently receiving care from the team.

4. The Practice, on behalf of each Practice physician and any other Authorized User, shall execute a License Agreement with Noteworthy. For purposes of this Agreement, Authorized User is defined as any employee, contractor or agent designated by the Practice to be given passwords, User IDs, and any other authentication mechanisms necessary for them to access the Portal. The Practice will designate such "Authorized Users" based solely on the "need to know" related to treatment of specific patients. Use of the data obtained through the Portal by persons who are not Authorized Users or by Authorized Users for purposes other than direct patient care is strictly prohibited and may result in termination as an HIE Participant.

5. The Coalition and the Practice shall cooperate in the training of all HIE Participants regarding the implementation and use of the Portal and the HIE Participation Criteria.

6. The Practice agrees to procure and maintain, at Practice's sole cost, any technology, hardware, telecommunication lines and Internet service connections necessary to use the Portal.

7. The Practice shall comply, and shall require its Authorized Users to agree in writing that they are legally bound to comply, with the HIE Participation Criteria. Failure by the Practice, or its Authorized Users, to comply with such criteria may result in termination as an HIE Participant.

8. The Practice agrees to maintain software configuration settings with the Portal that permits the sharing of the Practices' data with other HIE participants within and outside of the Practice subject to the HIE Participation Criteria.

9. The Practice shall monitor use of the Portal by its Authorized Users and shall be solely responsible, with respect to the use of the HIE interface and/or patient data used or disclosed in connection therewith, for all acts and omissions of the Practice or its Authorized Users, and any other individuals who may access or use the HIE interface either through the Practice or by use of any password, identifier of log-on received or obtained, directly or indirectly, lawfully or unlawfully, from the Practice or any of its Authorized Users.

10. The Practice shall be solely responsible for obtaining consent from its patients under all current federal and state laws and all amendments thereto and any policy which the Coalition may implement, with respect to the use of Protected Health Information, as that term is defined under 45 C.F.R. § 160.103.

11. Patient Care. The Practice shall be solely responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for their respective patients and clients resulting from or in any way related to the use of the Portal or patient data. Neither the Practice nor any Authorized User shall have any recourse against, and shall waive, any claims against the Coalition for any loss, damage, claim, or cost relating to or resulting from its own use or misuse of any patient data.

12. The Coalition may terminate an HIE Participant in accordance with the termination provisions at Section G of the Agreement. The Coalition may also terminate HIE Participation if it terminates its Marketing and Services Agreement with Noteworthy. Termination of HIE Participation shall not terminate the Collaborative Services Agreement.

13. The Practice may be temporarily prevented from accessing the HIE Data by the Coalition if there is a reasonable belief that the Practice or its Authorized User/s are not in compliance with this Participation Agreement or the HIE Participation Criteria. Furthermore, the Practice may be terminated from Participation in the HIE if any Practice or its Authorized User/s remains non-compliant under the terms of this Participation Agreement or the HIE Participation Criteria.

14. The Practice is not required to use the Portal for any particular patient. In order for the Coalition to allocate efficiently Grant funds for implementation of the HIE, however, the Practice agrees to use the HIE Portal for purposes of obtaining data relevant to the Practice's patients at least twice per month.

15. The Practice will ensure that the Coalition has a correct email address for all Authorized Users and that the Coalition will be notified by email at **info@CamdenHealth.org** within two (2) business days of termination of an Authorized User from employment by the Practice.

IN WITNESS WHEREOF, the parties, through their duly authorized officers, have executed this Participation Agreement effective as of the Effective Date.

PRACTICE	**CAMDEN COALITION OF HEALTHCARE PROVIDERS**
By: ______________________________	______________________________
Print Name: ______________________	______________________________
Print Title: _______________________	______________________________
Date: _________________________	______________________________

Addendum

Camden HIE Participation Criteria

1. HIE Participants will access the HIE Portal and use data from the HIE Portal solely for treatment of specific patients and not for any other purpose.

2. HIE Participants shall comply with all applicable laws when accessing data through the HIE Portal, including without limitation HIPAA regulations and any other privacy and security-related requirements, federal and state breach reporting requirements, fraud and abuse requirements, and licensure requirements.

3. HIE Participants acknowledge that the Practice, in cooperation with the Coalition, shall monitor use of the HIE Portal by its HIE Participants and notify the Coalition immediately in writing regarding any inappropriate use of the HIE Portal and any inappropriate use and disclosure of data from the HIE Portal, including without limitation any Security Incident or Security Breach as defined under the HIPAA regulations and DHHS rules regarding Breach Notification for Unsecured Protected Health Information. Furthermore, the Practice shall cooperate with the Coalition to notify all parties, as applicable, in the event of a security breach.

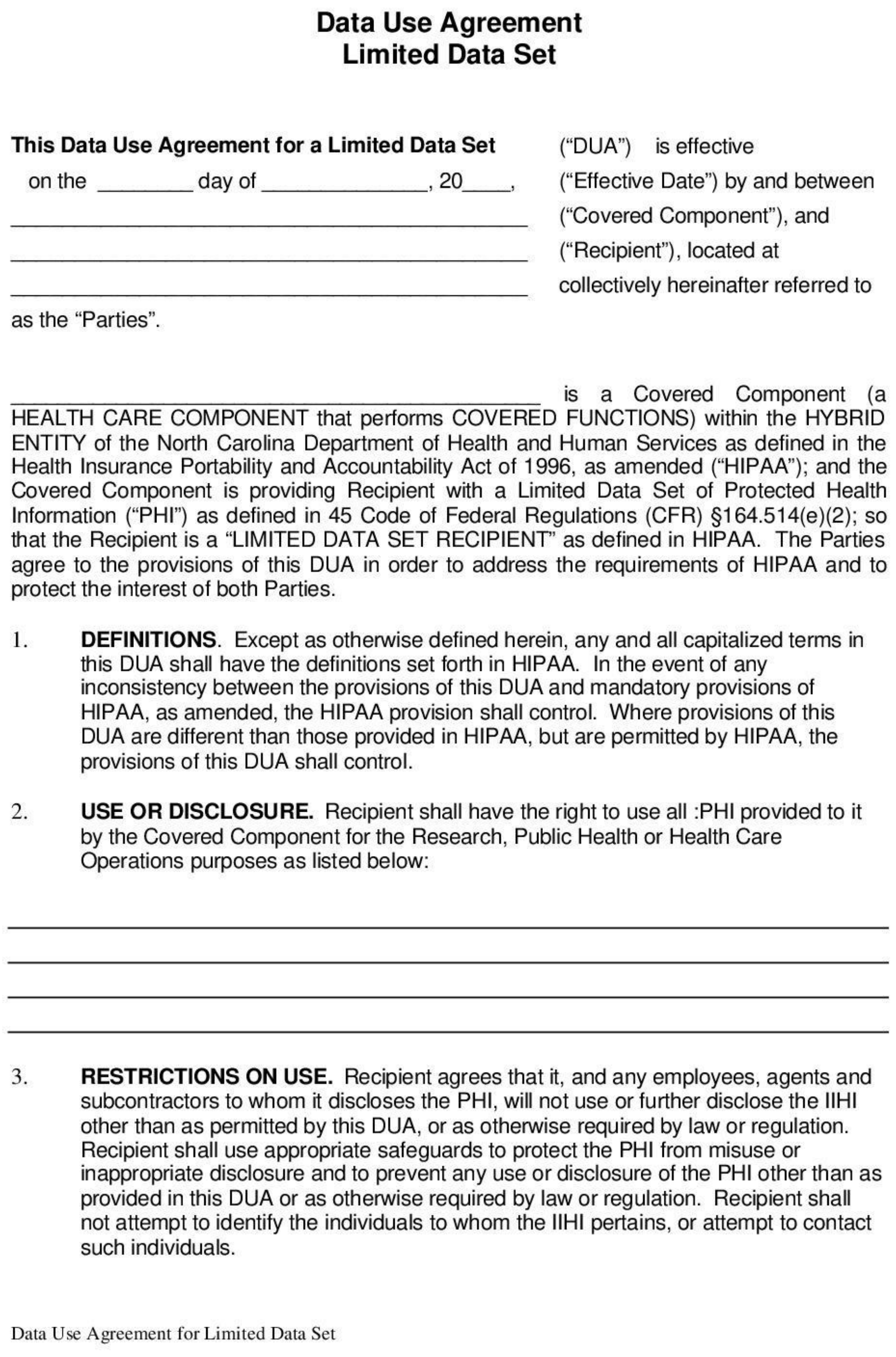
4. HIE Participants acknowledge that any HIE Participant (as well as any person who accesses the Portal or Portal information without authorization) who violates these Participation Criteria in accordance with applicable law, including without limitation the HIPAA regulations may be disciplined in accordance with the Practice's policies for non-compliance, as applicable, and may be prohibited from access to the HIE Portal.

5. HIE Participants acknowledge that the Practice authorizes Noteworthy to share with the Coalition information regarding the Practice's use of the HIE Portal, including without limitation any audit trail information, in order for the Coalition to review HIE participation and administration generally, and to determine whether its HIE Participants have complied with these HIE Participation Criteria.

6. HIE Participants acknowledge that the Coalition may revise these HIE Participation Criteria from time to time, provided that the Coalition shall notify the Practice of any such change at least thirty (30) days prior to the implementation of the change.

7. In order to access the HIE Portal, an HIE Participant shall have and maintain appropriate licensure/registration, as required in the state of New Jersey, and shall not be subject to any disciplinary restrictions, nor shall they have been excluded or debarred from participation in any government payor program.

Sample Data Usage Agreement



Data Use Agreement
Limited Data Set

This Data Use Agreement for a Limited Data Set ("DUA") is effective
on the ________ day of ______________, 20____, ("Effective Date") by and between
____ ("Covered Component"), and
____ ("Recipient"), located at
____ collectively hereinafter referred to
as the "Parties".

____ is a Covered Component (a HEALTH CARE COMPONENT that performs COVERED FUNCTIONS) within the HYBRID ENTITY of the North Carolina Department of Health and Human Services as defined in the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"); and the Covered Component is providing Recipient with a Limited Data Set of Protected Health Information ("PHI") as defined in 45 Code of Federal Regulations (CFR) §164.514(e)(2); so that the Recipient is a "LIMITED DATA SET RECIPIENT" as defined in HIPAA. The Parties agree to the provisions of this DUA in order to address the requirements of HIPAA and to protect the interest of both Parties.

1. **DEFINITIONS**. Except as otherwise defined herein, any and all capitalized terms in this DUA shall have the definitions set forth in HIPAA. In the event of any inconsistency between the provisions of this DUA and mandatory provisions of HIPAA, as amended, the HIPAA provision shall control. Where provisions of this DUA are different than those provided in HIPAA, but are permitted by HIPAA, the provisions of this DUA shall control.

2. **USE OR DISCLOSURE.** Recipient shall have the right to use all :PHI provided to it by the Covered Component for the Research, Public Health or Health Care Operations purposes as listed below:

____

____

____

____

3. **RESTRICTIONS ON USE.** Recipient agrees that it, and any employees, agents and subcontractors to whom it discloses the PHI, will not use or further disclose the IIHI other than as permitted by this DUA, or as otherwise required by law or regulation. Recipient shall use appropriate safeguards to protect the PHI from misuse or inappropriate disclosure and to prevent any use or disclosure of the PHI other than as provided in this DUA or as otherwise required by law or regulation. Recipient shall not attempt to identify the individuals to whom the IIHI pertains, or attempt to contact such individuals.

4. **REPORTING**. Recipient shall report to Covered Component any use or disclosure of the PHI that is not provided for in this DUA of which the Recipient becomes aware. Recipient will take reasonable steps to limit any further such use or disclosure.

5. **TERM AND TERMINATION.**

(a) Term. The Term of this DUA shall be effective as of the date first written above, and shall terminate when all the PHI provided by Covered Component to Recipient is destroyed or returned to Covered Component, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination for Cause. Should Recipient commit a material breach of this DUA, which is not cured within thirty (30) days after Recipient receives notice of such breach from the Covered Component, then the Covered Component will discontinue disclosure of PHI and will report the problem to the Secretary, U. S. Department of Health and Human Services.

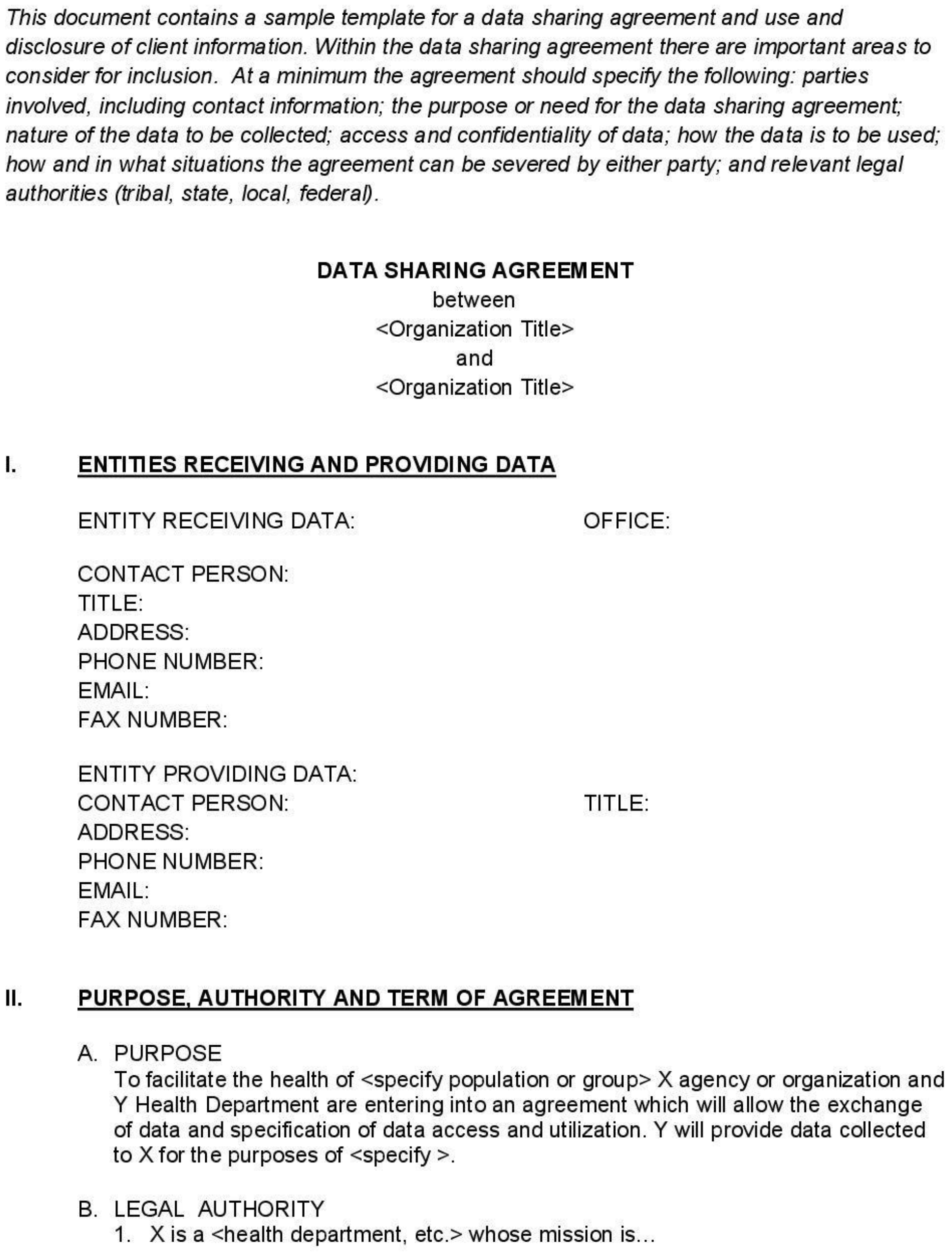
(c) Effects of Termination.

i. Except as provided in paragraph (ii) of this subsection, within ten (10) days upon termination of this DUA, Recipient shall return or destroy all PHI received from Covered Component. This provision shall apply to PHI that is in the possession of subcontractors or agents of Recipient. Recipient shall retain no copies of the PHI.

ii. In the event that Recipient determines that returning or destroying the PHI is infeasible, Recipient shall provide to Covered Component notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of PHI is infeasible, Recipient shall extend the protections of this DUA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Recipient maintains PHI.

COVERED COMPONENT:	RECIPIENT:
______________________________ *(Date)*	______________________________ *(Date)*
______________________________ *(Signature)*	______________________________ *(Signature)*
______________________________ *(Printed Name)*	______________________________ *(Printed Name)*
______________________________ *(Title)*	______________________________ *(Title)*

Sample Data Sharing Agreement



This document contains a sample template for a data sharing agreement and use and disclosure of client information. Within the data sharing agreement there are important areas to consider for inclusion. At a minimum the agreement should specify the following: parties involved, including contact information; the purpose or need for the data sharing agreement; nature of the data to be collected; access and confidentiality of data; how the data is to be used; how and in what situations the agreement can be severed by either party; and relevant legal authorities (tribal, state, local, federal).

DATA SHARING AGREEMENT
between
<Organization Title>
and
<Organization Title>

I. ENTITIES RECEIVING AND PROVIDING DATA

ENTITY RECEIVING DATA: OFFICE:

CONTACT PERSON:
TITLE:
ADDRESS:
PHONE NUMBER:
EMAIL:
FAX NUMBER:

ENTITY PROVIDING DATA:
CONTACT PERSON: TITLE:
ADDRESS:
PHONE NUMBER:
EMAIL:
FAX NUMBER:

II. PURPOSE, AUTHORITY AND TERM OF AGREEMENT

A. PURPOSE
To facilitate the health of <specify population or group> X agency or organization and Y Health Department are entering into an agreement which will allow the exchange of data and specification of data access and utilization. Y will provide data collected to X for the purposes of <specify >.

B. LEGAL AUTHORITY
1. X is a <health department, etc.> whose mission is…

2. Y is an <organization, agency, health department, etc.> whose mission is for public benefit.

C. PERIOD OF PERFORMANCE
This Agreement shall be effective when signed by both parties and shall continue until terminated pursuant to the termination clause contained herein.

III. DESCRIPTION OF DATA/DATA WORKPLAN

The following data will be provided under this agreement: <list of specific data items and agreement parameters>

If applicable, all data generated by this project shall be approved for dissemination by the <specific IRB> Institutional Review Board and <any other relevant approvals, including health departments>.

IV. ACCESS TO DATA

A. METHOD OF ACCESS AND TRANSFER
Data will be obtained and/or accessed in the following manner:

B. PERSONS HAVING ACCESS TO DATA
All persons who will have access to data must complete a data privacy training through < specify >.
Prior to the transfer of any data, staff members and researchers who will have access to the data shall sign <relevant confidentiality statement/assurances>, (signed copies shall be provided to X).

C. FREQUENCY OF DATA EXCHANGE
Data will be exchanged as needed to meet reporting requirements as well as on an ongoing basis between X and Y staff for the entire length of the project.

V. SECURITY OF DATA

Datasets containing protected health information (PHI) shall be encrypted or otherwise protected as specified. All reasonable precautions shall be taken to secure the data from individuals who do not specifically have authorized access. Data shall be kept on a password-protected file server located in a secure environment. Data will be kept in a separate directory on server which is also password-protected and will be accessible only by Y evaluators or staff members specifically authorized access as provided in this Agreement.

VI. CONFIDENTIALITY

A. REGULATIONS COVERING CONFIDENTIALITY OF DATA

The use and disclosure of information obtained under this contract shall be subject to <specific legal authority>. X and Y shall maintain the confidentiality of any information which may, in any manner, identify individual subjects.

Confidentiality of all data must be ensured.

B. NON-DISCLOSURE OF DATA
Y shall not disclose, in whole or in part, the data described in this agreement to any individual or agency not specifically authorized by this agreement.

Data shall be provided on a timely basis. Y will document uses and users of the data and will report this information routinely back to the X <designated official>.

C. Y will not disclose directly to, or use for the benefit of, any third party confidential information, knowledge or data acquired by virtue of its relationship with the other party named in this Agreement, without the prior written approval of the other party. It is understood and agreed by the parties that the obligations of this paragraph shall survive the expiration of termination of this Agreement.

VII. <u>PROPERTY RIGHTS</u>

Original materials prepared by Y, including, without limitation: reports, proposals, analysis, writings, sound recordings, pictorial reproductions or materials of any type whatsoever, are and shall remain the <sole and exclusive or joint property> of <stipulate organization, or health department>. Y will assert no right, claim or interest of any nature whatsoever with respect thereto, including specifically but, without limitation, any claim to statutory copyright.

Data Use and Ownership

X shall be cited as the source of the data in all tables, reports, presentations, and scientific papers, and Y shall be cited as the source of interpretations, calculations, and/or manipulations of the data.

VIII. <u>SEVERABILITY</u>

If any provision of this Agreement or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision, if such remainder conforms to the requirement of applicable law and the fundamental purpose of this agreement, and to this end the provisions of this Agreement are declared to be severable.

IX. <u>TERMINATION</u>

Either party may terminate this Agreement upon 30 days prior written notification to the other party.

X. **RIGHT OF INSPECTION**

Y shall provide X the right of access to its facilities at all reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance under this contract.

XI. **ALL WRITINGS CONTAINED HEREIN**

This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind any of the parties hereto.

Organization X <health department>

________________________________ ______________________
Name/Title Date

________________________________ ______________________
Name/Title Date

Organization Y <agency/health department receiving data>

________________________________ ______________________
Name/Title Date

________________________________ ______________________
Name/Title Date

USE AND DISCLOSURE OF CLIENT INFORMATION

Staff with access to confidential client information are responsible for understanding rules for use rules of behavior with respect to disclosure of the information. Outlined below are key elements for staff to remember:

A. CONFIDENTIALITY OF CLIENT DATA

1. Individually identifiable patient data is confidential and is protected by various state and federal laws.
2. Confidential patient information includes all personal information (e.g., name, birth date, social security number, diagnosis, treatment, etc.) which may, in any manner, identify the individual.

B. USE OF CLIENT DATA

1. Client data may be used only for purposes directly described in the data sharing agreement between X and Y
2. Any personal use of patient information is strictly prohibited.
3. Access to data must be limited to those staff whose duties specifically require access to such data in the performance of their assigned duties.

C. DISCLOSURE OF INFORMATION

1. Identified patient information may not be disclosed to other individuals or agencies.
2. Questions related to disclosure are to be directed to X.
3. Any disclosure of information contrary to 1 above is unauthorized and is subject to penalties identified in law.

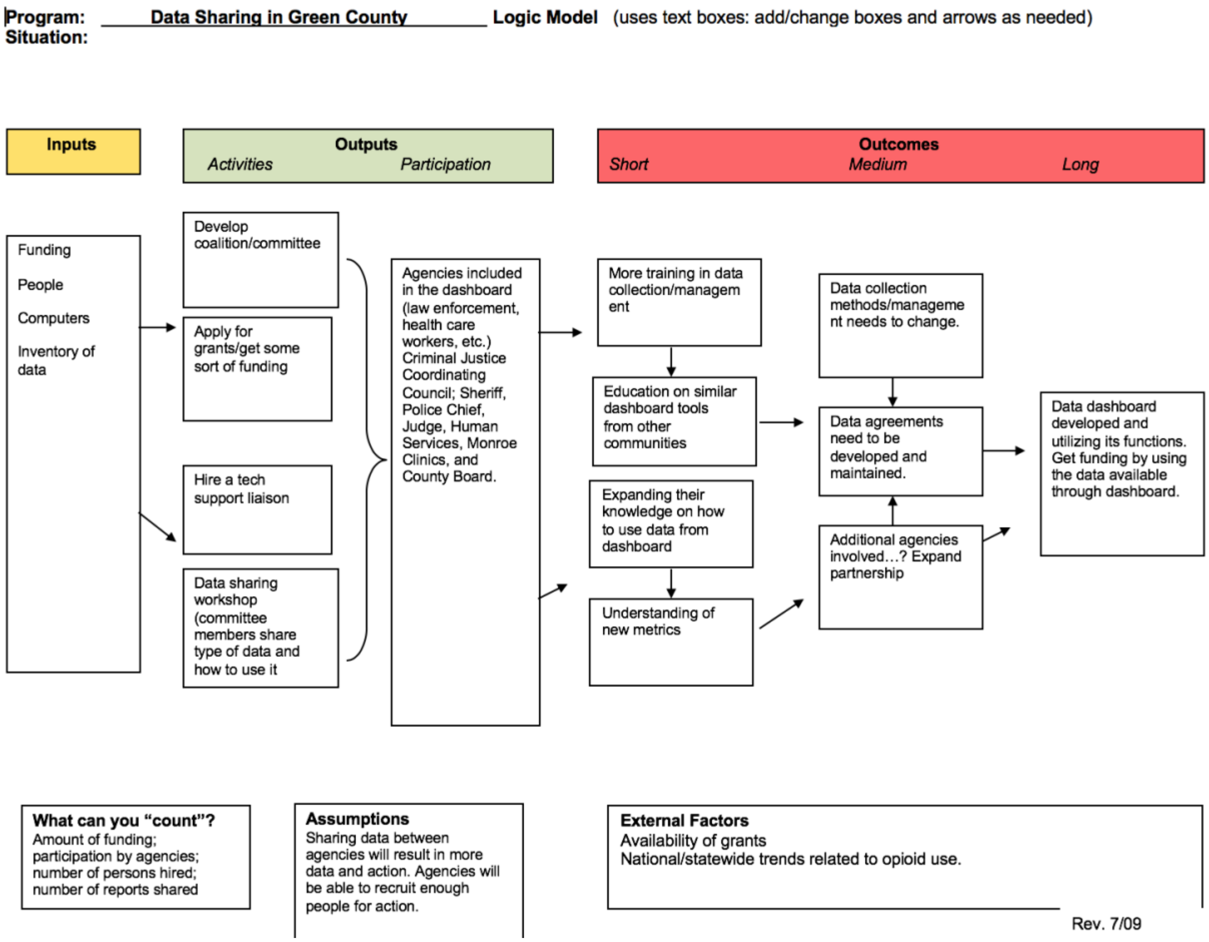
Name (print): ______________________________

Signature: ______________________________ Date:_____________

Approved By: ______________________________
Authorizing Official, X <health department>

Signature: ______________________________ Date:_____________

Appendix C: Logic Model



Program: **Data Sharing in Green County** **Logic Model** (uses text boxes: add/change boxes and arrows as needed)
Situation:

Inputs

Outputs
Activities *Participation*

Outcomes
Short *Medium* *Long*

Funding

People

Computers

Inventory of data

Develop coalition/committee

Apply for grants/get some sort of funding

Hire a tech support liaison

Data sharing workshop (committee members share type of data and how to use it

Agencies included in the dashboard (law enforcement, health care workers, etc.) Criminal Justice Coordinating Council; Sheriff, Police Chief, Judge, Human Services, Monroe Clinics, and County Board.

More training in data collection/management

Education on similar dashboard tools from other communities

Expanding their knowledge on how to use data from dashboard

Understanding of new metrics

Data collection methods/management needs to change.

Data agreements need to be developed and maintained.

Additional agencies involved…? Expand partnership

Data dashboard developed and utilizing its functions. Get funding by using the data available through dashboard.

What can you "count"?
Amount of funding; participation by agencies; number of persons hired; number of reports shared

Assumptions
Sharing data between agencies will result in more data and action. Agencies will be able to recruit enough people for action.

External Factors
Availability of grants
National/statewide trends related to opioid use.

Rev. 7/09

About UniverCity Year

UniverCity Year is a three-phase partnership between UW-Madison and one community in Wisconsin. The concept is simple. The community partner identifies projects that would benefit from UW-Madison expertise. Faculty from across the university incorporate these projects into their courses, and UniverCity Year staff provide administrative support to ensure the collaboration's success. The results are powerful. Partners receive big ideas and feasible recommendations that spark momentum towards a more sustainable, livable, and resilient future. Join us as we create better places together.

GREEN
COUNTY
WISCONSIN

UniverCity Alliance
UNIVERSITY OF WISCONSIN–MADISON

universityalliance@wisc.edu
608-890-0330
univercity.wisc.edu