Case Study Report

The Kentucky Health Information Data Sharing Project

Sharing Healthcare Data with Child Welfare Workers to Improve the Well-being of Children in Foster Care

November 2023

A resource tool from the
ACF Interoperability Initiative

Case Study Report

The Kentucky Health Information Data Sharing Project: Sharing Healthcare Data with Child Welfare Works to Improve the Well-being of Children in Foster Care

OPRE Report 2023-298

November 2023

Mary Gabay and Frank Bennici, Westat.

Submitted to:
Aaron Goldstein, Project Officer
Office of Planning, Research, and Evaluation
Administration for Children and Families
U.S. Department of Health and Human Services

Contract Number: HHSP233201500671

Project Director: Janice Machado
Westat
1600 Research Blvd.
Rockville, MD 20850

This report and other reports sponsored by the Office of Planning, Research, and Evaluation are available at www.acf.hhs.gov/opre.

Acknowledgements

The authors are grateful for the opportunity and guidance provided by the Administration for Children and Families, in particular Aaron Goldstein and Brett Brown. We would like to thank everyone associated with the Kentucky Health Information Data Sharing (KHIDS) Project who gave their time to be interviewed for this case study:

Dr. Matthew Walton, Research Scientist, Office of Data Analytics, Kentucky Cabinet for Health and Family Services

Andrew Bledsoe, Deputy Executive Director, Kentucky Health Information Exchange

Kathleen Hines, Chief Privacy Officer, Kentucky Cabinet for Health and Family Services

Amy Smith, Executive Staff Advisor, Privacy Program, Kentucky Cabinet for Health and Family Services

Pamela Wright, Program Manager, Office of Data Analytics, Kentucky Cabinet for Health and Family Services

Tracy DeSimone, Assistant Director, Division of Protection and Permanency, Kentucky Department for Community Based Services

Mary Carpenter, Director, Division of Protection and Permanency, Kentucky Department for Community Based Services

We would also like to thank Devan McGraw**,** a member of our expert panel, who provided important feedback on this document.

The views expressed in this publication do not necessarily reflect the views or policies of the expert panel, contributors, Office of Planning, Research, and Evaluation, Administration for Children and Families, or the U.S. Department of Health and Human Services.

DISCLAIMERS:

- This case study report is not official legal or regulatory guidance, and to the extent there is any conflict between this case study and regulations or laws, those regulations and laws take precedence.
- The views expressed in this publication do not necessarily reflect the views or policies of the Office of Planning, Research, and Evaluation, the Administration for Children and Families, or the U.S. Department of Health and Human Services.

Executive Summary

The Administration for Children and Families (ACF) Office of Planning, Research, and Evaluation (OPRE) is sponsoring a project to create a set of tools that ACF, states, localities, and tribes can use when developing data sharing initiatives while protecting the data privacy and confidentiality of service recipients. This case study of the Kentucky Health Information Data Sharing (KHIDS) Project is among this set of tools; it is intended for agency leadership and program officials who want to implement or improve a similar data sharing initiative.

The Kentucky Cabinet for Health and Family Services (CHFS) manages most of Kentucky's human services and healthcare programs. The CHFS agency overseeing the well-being of foster children in Kentucky recognized their child welfare workers (CWWs) could not efficiently acquire a foster child's healthcare records and coordinate their care. They also recognized another CHFS agency managed an information system that allows healthcare providers in Kentucky to exchange electronic real-time patient healthcare records. CHFS and several of its agencies decided to develop the KHIDS interface, a system-to-system connection that would give CWWs access to those electronic real-time patient healthcare records.

Before implementing the KHIDS interface CHFS and its agencies worked through several challenges including:

- Modifying the current child welfare information system to directly access the healthcare information system so it would be more convenient for CWWs to find the records they needed.
- Determining when federal and state privacy laws permitted CWWs to access the records.
- Developing agreements so the parties that shared and received the patient healthcare records data knew their responsibilities and expectations with respect to the data sharing.
- Implementing controls to assure CWWs would access and use the healthcare records appropriately.

The interviewees for this case study identified lessons learned and recommendations from their work with the KHIDS interface. These focus on issues of data privacy and confidentiality but include other aspects of development that helped encourage the success of the KHIDS Project. The information the interviewees would provide to others who are seeking to build a similar system include:

- Ensure that your privacy officer is involved right from the beginning. These systems involve the sharing of sensitive and confidential data. To protect the data from inappropriate access, your privacy officer may require changes to your initial plans. Knowing from the start what your privacy officer will and will not allow will help you avoid the additional time and cost associated with making changes after work on the system has already begun.

- Engage all possible collaborators and system users at the start of a project to help facilitate project implementation. When interested parties are involved in a project from the beginning, they are more likely to understand the project and how the data will be used, which makes it easier to work with them to complete the necessary agreements and get the project off the ground. By comparison, if you start the project in a silo, then find you need to engage another party, they will be new to the project, and it may take additional time to acquire their support. A solution is to engage all parties that may be involved in, and affected by, the project from the beginning, even if there is a chance that party may not actually need to be involved.

- The training given to system users is an important part of the overall system implementation. All relevant leaders, program personnel, and intended users, including the privacy officer, should review training materials to ensure it will teach trainees about the system and how to use it.

- Include a robust evaluation piece in your project. Evaluating system utilization will let you know what users need (if anything) to make better use of the system. The lessons KHIDS leaders and partners learned by evaluating system utilization were helpful in improving the process. Eventually evaluators hope to show whether increased system utilization improves the well-being of DCBS's foster children.

Table of Contents

Page

Acronyms

ACF	Administration for Children and Families
CHFS	Cabinet for Health and Family Services
CPO	Chief Privacy Officer
CWW	Child Welfare Worker
DCBS	Department for Community Based Services
DMS	Department for Medicaid Services
HIPAA	Health Insurance Portability and Accountability Act
HSII	Human Services Interoperability Innovations
KHIDS	Kentucky Health Information Data Sharing Project
KHIE	Kentucky Health Information Exchange
MOU	Memorandum of Understanding
ODA	Office of Data Analytics
OPRE	Office of Planning, Research, and Evaluation
TWIST	The Worker Information System

Introduction

The Administration for Children and Families (ACF) Office of Planning, Research, and Evaluation (OPRE) is sponsoring a project to create a set of tools that ACF, states, localities, and tribes can use when developing data sharing initiatives while protecting the data privacy and confidentiality of service recipients. This case study is among this set of tools; it is intended for agency leadership and program officials who want to implement a new data sharing initiative or improve or expand an existing initiative. It discusses a particular data sharing initiative implemented to provide child welfare workers (CWWs) access to the healthcare records of the foster children they serve. This report also highlights data privacy and confidentiality challenges encountered and resolved during project implementation, and includes advice from the individuals who participated in the initiative.

The Kentucky Health Information Data Sharing (KHIDS) Project provided CWWs easier access to healthcare records of the foster children they serve. This was done via an interface that connected two information systems managed by two different parts of the Kentucky Cabinet for Health and Family Services (CHFS):

- Kentucky Health Information Exchange (KHIE), a healthcare records information system managed by the CHFS Department for Medicaid Services (DMS) and
- The Worker Information System (TWIST), a child welfare information system managed by the CHFS Department for Community Based Services (DCBS).

The resulting data share will improve the health and well-being of foster children in Kentucky and increase the efficiency with which CWWs can do their work.

The project team selected the KHIDS Project for a case study because of its focus on child welfare—a priority topic area for this project. It also provides an important example of how an organization's chief privacy officer can influence the design and implementation of a data sharing initiative.

Sources of information for this case study include interviews with the Kentucky Cabinet for Health and Family Services (CHFS) staff, documents provided by those interviewed staff, and various resources identified through internet searches.

Motivation for Data Sharing

The State of Kentucky had 8,369 children in foster care as of September 30th, 2021.[1] These children can have complex healthcare needs that require significant time and effort to manage appropriately. Over time, they can also have multiple placements, which may be in different counties with different doctors. Simply determining whether a foster child had a check-up in the previous year can take hours of work. Coordinating a foster child's overall healthcare can involve CWWs and others "calling physician offices for release of information forms, driving

[1] Children's Bureau Child Welfare Outcomes State Data Review Portal website: https://cwoutcomes.acf.hhs.gov/cwodatasite/pdf/kentucky.html. Accessed on 9/18/2023.

across the state for doctor visits, filling out prior authorization forms to get medication filled at pharmacies, tracking down records of past medical procedures, and navigating several other logistical processes."[2]

Kentucky recognized that giving CWWs easier access to healthcare records of the foster children they serve would reduce this time and energy burden, allowing CWWs to spend more time on other important tasks. Kentucky recognized that many of the healthcare records about these foster children were already maintained in KHIE. However, Kentucky also recognized that giving CWWs direct access to KHIE needed to occur in an efficient, legal, and responsible manner.

In 2020, Kentucky received a $600,000 Human Services Interoperability Innovations (HSII) grant from ACF to help develop an interface to provide CWWs direct access. The HSII demonstration program is "intended to expand data sharing efforts by state, local, and tribal governments to improve human services program delivery, and to identify novel data sharing approaches that can be replicated in other jurisdictions."[3] Kentucky hoped direct access would eliminate the challenges CWWs experienced when trying to acquire healthcare records (e.g., time and effort), improve coordination, and ultimately improve the health and well-being of Kentucky's foster children.

Participating Offices

Kentucky's Cabinet for Health and Family Services (CHFS) manages most of Kentucky's human services and healthcare programs. This project involved several CHFS agencies:

- The Department for Medicaid Services (DMS) is Kentucky's Medicaid agency. Among other roles, DMS (a) provides Medicaid to all of Kentucky's foster children, (b) received the grant from HSII to develop the KHIDS interface, and (c) is responsible for the Medicaid records shared via the interface.

- The Department for Community Based Services (DCBS) administers Kentucky's child welfare program. Among other roles, DCBS manages and trains the CWWs who can access healthcare records through the KHIDS interface.

- The Office of Data Analytics (ODA)[4] includes three Divisions that are key to this project.
    - The Division of Analytics monitored and evaluated the HSII grant, which included a survey of CWWs and their use of the KHIDS interface.
    - The Division of Health Information operates KHIE.

---

[2] Kentucky Cabinet for Health and Family Services. *Human Services Interoperability Innovation to Improve Health Services for Youth in Foster Care in Kentucky: The Kentucky health Information Data Sharing (KHIDS) Project*. Grant white paper.

[3] Human Services Interoperability Innovations (HSII) website: https://www.acf.hhs.gov/opre/project/human-services-interoperability-innovations-hsii-2020-2021. Accessed on 9/18/2023.

[4] This office was called the Office of Health Data and Analytics (OHDA) until July 2022.

    - The CHFS Privacy Office analyzed the relevant privacy laws and helped ensure the KHIDS interface met those requirements.

- The Office of Application Technology Services provides information technology support to CHFS, administers TWIST, and provided the technical expertise to build and install the KHIDS interface.

The Information Systems

Kentucky's solution was to develop the KHIDS interface so CWWs could efficiently acquire the healthcare records of the foster children they serve. This section describes the two information systems and the interface; later sections describe the privacy controls established to assure the CWWs access and use the healthcare records appropriately.

The Worker Information System (TWIST)

TWIST is Kentucky's child welfare information system. It has approximately 2,700 users and exchanges data with select partners including the courts and Kentucky Department of Education. Among other features, if a child in Kentucky is placed outside their home, TWIST can collect records about the child and their placement, remind CWWs when to complete certain tasks, and give program managers an overview of each child's status.[5]

The information that TWIST maintains about Kentucky's child welfare population includes:

- referrals and assessments of maltreatment to include data on victims, perpetrators, issues of safety, and determination on the referral;
- demographic characteristics of children and adults;
- entry and exit data for children placed in foster care;
- plans for services and permanency;
- court activities;
- Title IV-E determinations;
- contacts with case participants; and
- ongoing case management activities including adoption activities such as placement and finalized adoptions.[6]

[5] See https://www.fosteringcourtimprovement.org/CFSR/CFSR2Reports/KY/CFSRFinalReport1stRoundCFSR.pdf, page 49. Accessed on 9/18/2023.

[6] Department for Community Based Services, Division of Protection and Permanency. Kentucky Child and Family Services Plan, 2020 – 2024. https://www.chfs.ky.gov/agencies/dcbs/dpp/cpb/Documents/ChildFamilyServicePlan.pdf. Accessed on 9/18/2023.

Kentucky Health Information Exchange (KHIE)

KHIE is an information system that allows healthcare providers in Kentucky to exchange electronic real-time patient healthcare records safely and securely.[7] Among other uses, if a patient visits a Kentucky healthcare provider, the provider can see information about that patient collected by other Kentucky healthcare providers.

Kentucky healthcare providers can use KHIE if they use an electronic health record system and sign a participation agreement. A recent environmental scan found that all but one hospital in Kentucky actively sends data to KHIE. The KHIE team also estimates that about 82 percent of Kentucky's ambulatory providers and about 86 percent of Kentucky's Medicaid providers use KHIE.

The healthcare providers who use KHIE can transmit and receive:

- patient demographics;
- lab and pathology results;
- transcribed reports including radiology;
- immunization data;
- summaries of care;
- facility admission, discharge, and transfer data;
- behavioral health data; and
- data from emergency medical services and correctional facilities.

Not all providers who use KHIE transmit all this data; smaller providers may only transmit immunization data or COVID-19 test results.

Kentucky Health Information Data Sharing (KHIDS) Interface

The KHIDS interface connected KHIE to TWIST so CWWs could efficiently acquire the healthcare records of the foster children they serve. TWIST was modified so CWWs now see a link to KHIE (a) on the home page and (b) any time they access a foster child's case record. If they click that link and accept the terms and conditions that appear, they open a KHIE web-based portal called *ePartnerViewer*.[8]

ePartnerViewer allows CWWs to access all the information KHIE collected about a foster child. An "at a glance" summary shows the most recent information and other information the CWW may consider most relevant. *ePartnerViewer* also proactively notifies the CWW if anyone they are serving experienced a key event, such as being discharged from an emergency department or a receiving a positive COVID-19 test result.

CWWs noted two issues with the KHIDS interface. The bigger issue is the number of providers who do not transmit all the data that KHIE can collect. The DCBS nurses who work with medically complex children said they appreciate having access to more information, but at least

[7] Additional information about KHIE can be found at https://khie.ky.gov/Participants/Pages/All-KHIE-Participants.aspx. Accessed on 9/18/2023.

[8] See https://khie.ky.gov/epartner-viewer/Pages/default.aspx. Accessed on 9/18/2023.

some of the information they would like to access is not transmitted to KHIE. This has made the interface less beneficial to CCWs than it could be. The second issue is that CWWs without healthcare backgrounds sometimes have difficulty reading and understanding the more technical clinical information available through the interface.

Navigating the Applicable Laws

Several state and federal privacy laws govern who may access the healthcare records maintained in KHIE and when. The CHFS Chief Privacy Officer (CPO) was responsible for identifying those laws and determining if they would allow CWWs to access the records of the foster children they serve. The CPO ultimately determined that CWWs could access those healthcare records in certain situations.

In particular, the CPO found that Kentucky Revised Statute 620.230 (KRS 620.230) permits CWWs to access the healthcare records of a child in DCBS custody. It says Kentucky foster children must have a case permanency plan which includes: *A description of the type of home, child-caring facility, child-placing agency or facility in which the child is to be placed or has been placed, and a statement why the placement is appropriate for the child, including but not limited to:…medical needs…*[9] The CPO reasoned that:

- CWWs are responsible for creating a permanency plan when they place a foster child;
- the permanency plan must consider whether a placement matches the child's medical needs; and
- the CWW needs the child's healthcare records to determine those medical needs.

Interestingly, KRS 620.230 did not explain how CWWs should obtain the healthcare records, nor does it say that healthcare providers must share the healthcare records with the CWWs.

The CPO found that the federal Social Security Act Title IV-E (Title IV-E) permits CWWs to access healthcare records about a child in DCBS custody. Title IV-E applies to DCBS because DCBS receives certain Title IV-E funds. Like KRS 620.230, Title IV-E says foster children must have a case plan which considers their medical conditions. This includes: *…the most recent information available regarding—(iv) a record of the child's immunizations; … (v) the child's known medical problems; (vi) the child's medications; and (vii) any other relevant health and education information concerning the child determined to be appropriate by the State agency.*[10] Again, the CPO reasoned that CWWs need the child's healthcare records to accomplish this.

The CPO also found that the federal Health Insurance Portability and Accountability Act (HIPAA) regulations permits CWWs to access the healthcare records of a child in DCBS custody. HIPAA applies to most healthcare records created by healthcare providers in the United

[9] Accessed at: https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=52818. Accessed on 9/18/2023.

[10] See Title IV-E of the Social Security Act (42 U.S.C. § 670 et seq.) and specifically 42 U.S.C. § 671(a)(16) at https://www.law.cornell.edu/uscode/text/42/671 and 42 U.S.C. § 675 at https://www.law.cornell.edu/uscode/text/42/675. Accessed on 9/18/2023.

States.[11] It says, in most situations, "a parent, guardian, or other person acting in loco parentis" of an unemancipated minor may make decisions about that minor's healthcare and access their healthcare records to make those decisions.[12] The CPO reasoned that, when a child is in foster care, DCBS and the appropriate CWWs are acting in loco parentis and should generally receive access to healthcare records.

The CPO did identify a few situations where Federal and Kentucky law allows minors to make decisions about their own healthcare and withhold that information from those acting in loco parentis.[13,14] This means CWWs should not access any records containing information about those decisions. Fortunately, healthcare providers are responsible for not uploading these records into KHIE, which means they should not appear in the KHIDS interface.

The CPO also had to navigate the fact that KHIE, as a Business Associate of DMS, could transmit data on behalf of Medicaid providers to other providers, but DCBS is not a healthcare provider and therefore could not sign a Participant Agreement with KHIE. To resolve this issue, the CPO recommended that DMS develop a separate agreement to share healthcare records with DCBS to coordinate healthcare services for foster children. The agreement would allow DCBS to serve as a named representative of the DMS and allow access to healthcare records through KHIE.

Legal Agreements

The parties that developed the KHIDS interface signed two overarching agreements to identify and acknowledge their responsibilities and expectations with respect to the interface—a Memorandum of Understanding (MOU) and a Business Associate Agreement. The appendices to this case study report include a copy of these agreements.

The MOU was signed by CHFS and all the agencies involved in the data sharing.[15] It says DMS will share the healthcare records in KHIE with DCBS-authorized CWWs to improve the coordination of care for foster children and deliver services in a "timely, appropriate, efficient, and cost-effective manner." It says a CWW may only access records belonging to a child who is both in DCBS custody and currently on that CWW's caseload. As noted above, there are situations where minors may make decisions about their own healthcare and withhold that information from those acting in loco parentis; the MOU says those records may not be shared through the KHIDS interface.

---

[11] See https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html. Accessed 9/18/2023.

[12] See https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html. Accessed on 9/18/2023.

[13] Key situations are discussed in the HIPAA Privacy Rule, 45 CFR 164.502(g), accessed at: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164#p-164.502(g). Accessed on 9/18/2023.

[14] Key situations are also discussed in Kentucky Revised Statute 214.185, accessed at https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=50969. Accessed on 9/18/2023.

[15] The CHFS agencies that were involved in the data sharing, and therefore signed the MOU, were DMS, DCBS, and ODA.

The Business Associate Agreement is the standard business associate agreement used by the DMS. It allows HIPAA covered entities such as DMS to share individually identifiable healthcare records with second parties (called "business associates") for a defined set of purposes. In this case, the covered entity is DMS and, by extension, DCBS, which is a named representative of DMS. The business associate is KHIE. The agreement delineates the obligations and activities expected of KHIE and describes permitted uses and disclosures of the protected health information transmitted to KHIE.

Child Welfare Worker Access Controls

The KHIDS interface has several controls in place to help assure CWWs will uphold the applicable privacy requirements, to incorporate privacy best practices, and to provide some flexibility when permitted. This includes controlling who accesses the KHIDS interface, and which records in KHIE they access.

Controlling Accesses to the KHIDS Interface

DCBS recognized many CWWs can access TWIST, but only some of them needed access to the healthcare records available through the KHIDS interface. Conveniently, TWIST already had a role-based access control system in place because that was required of all SACWIS systems.[16, 17] DCBS reviewed each role assigned to CCWs to determine whether CCWs with that role needed access to the KHIDS interface. DCBS generally decided a role needed access if those CCWs would directly interact with foster children or supervise those who do. For example, DCBS provided access to CWWs assigned to manage foster children or the healthcare services provided to foster children. DCBS often decided a role did not need access if those CWWs did not directly work with foster children. The CHFS CPO reviewed and approved each role that received access to the KHIDS interface.

DCBS will not provide a CWW access to the KHIDS interface until they complete a mandatory web-based training. That training remains available online in case CWWs want to review anything they learned. DCBS will also revoke a CWW's access to the KHIDS interface if they do not complete an annual refresher training. DCBS developed the training in collaboration with Eastern Kentucky University, and both the CPO and the CHFS Chief Information Security Officer reviewed and approved the content.

Controlling Access to the KHIE Records

The original design of the KHIDS interface would have given CWWs either access to all or none of the healthcare records in KHIE. The CPO rejected this design and suggested that CWWs only have access to the healthcare records of the children on their specific caseloads.

---

[16] In a role-based access control system, each user is assigned one or more system roles, which often closely corresponds to their role within the organization. The assigned roles determine what that user can access and do within the system. More information on how role-based access control systems operate and the benefits are available at https://csrc.nist.gov/projects/role-based-access-control. Accessed on 9/18/2023.

[17] See https://www.acf.hhs.gov/cb/training-technical-assistance/state-tribal-info-systems/historical-info for information on SACWIS systems.

Conveniently, TWIST already maintained a list of each CWW and the foster children they serve. Information technology staff developed a new feature which used those lists to limit access within the KHIDS interface. Specifically, whenever a CWW tries to access an individual's healthcare records, the KHIDS interface checks if that individual is a foster child served by that CWW. If yes, the CWW can access the individual's healthcare records. If not, the system denies access.

At the same time, the parties realized the lists might not always be updated, so they collaborated to develop the "break the glass" procedure. A CWW can access the healthcare records of someone who is not on their list (i.e., "break the glass") if they both:

- acknowledge they are requesting healthcare records for someone who is not on their list and
- enter a simple explanation as to why they are requesting access (e.g., the list was not yet updated, it was an emergency).

The system sends a daily and monthly report to KHIE, DCBS, and CPO administrative staff identifying each CWW who broke the glass, whose healthcare records they accessed, and the reason provided each time they broke the glass. On average, a monthly report contains about 120 instances. CPO staff review each monthly report, including the reasons given for breaking the glass, to make sure access has been appropriate. If anything causes a concern, they may try to determine why the CWW accessed the healthcare records and ask DCBS to investigate.

Originally the break the glass report contained many more instances. Many occurred because TWIST did not accurately reflect which foster children were served by which CWWs; CWWs needed to break the glass to see records about the foster children they served. This was solved by updating that information. Some instances occurred because a CWW would access a healthcare record on behalf of a coworker. For example, a coworker may ask for help because they did not have their computer. This is not an acceptable reason to break the glass and DCBS responded by further training the CWWs on when they were and were not permitted to break the glass.

Evaluating the KHIDS Project

KHIDS leaders realized that evaluating the KHIDS interface was an important part of the project. About a year after implementation, the ODA Division of Analytics launched a survey of CWWs to determine their impressions of the interface. The survey contained 18 questions that covered characteristics of the survey respondents, KHIDS utilization, and respondents' impressions of the KHIDS interface. It was open to the entire child welfare workforce and the results were publicly disseminated via a Research and Policy Brief.[18]

A total of 285 individuals answered some or all the survey questions. Of the 283 survey respondents who identified their role in DCBS, 35.0 percent were an "ongoing social service

[18] Conner, Kailyn L., Darby Todd, Cameron Bushling, and Matthew T. Walton. *Research and Policy Brief: Survey of Social Workers on Impressions of the KHIDS System*. Kentucky Cabinet for Health and Family Services, Office of Health Data and Analytics, Division of Analytics.

worker", 24.7 percent, were "Central Office staff", 20.5 percent were "family services office supervisors", 17.0 percent were "investigative social workers", and 2.8 percent were "service region staff." On average, respondents had worked for DCBS for 10 years, although the median number was 7 years. Unfortunately, it did not specifically ask if those respondents had used the KHIDS interface.

Not all survey respondents were aware they could access healthcare records for foster children through the new KHIDS interface. This was likely due to two reasons. One reason was worker turnover, which resulted in new staff that had not yet received training. A second reason was that, about one year after the KHIDS interface went live, it was still in an "adoption curve." CWWs were not required to use the KHIDS interface; they were only encouraged to use it if it was helpful to them. Use of the interface likely increased over time as "early adopters" spread the word about its usefulness. Of those survey respondents who reported using the interface, about one third said they used it at least once per week and a small number indicated they used it multiple times per day. The remaining two-thirds said they used the interface less than once per week, including a number of workers who had only used it a few times.

When workers did use the interface, they most commonly reported using it to:

- "make sure a child has been seen for well-child visits with a pediatrician" (27.5%);
- "verify that a child has been seen at an Emergency Room" (26.6%);
- "help a foster family access a healthcare service for their foster child" (24.8%); and
- "check alerts related to a child's COVID-19 test or diagnosis" (20.2%).

The alerts related to COVID-19 test results are part of a public health surveillance tool built into KHIE in response to the COVID-19 pandemic.

When asked about their general impressions of the KHIDS interface, most survey respondents who used the interface agreed (either somewhat or strongly) that it gave them access to important information needed to do their job well (61.8%). About half of these respondents agreed the KHIDS interface saved them time in their daily work (49.0%) and allowed them to provide better services to the foster children in their caseload (48.5%). However, a portion of the respondents who used the interface indicated they did not feel like they knew how to use the KHIDS interface well (21.6%) and were apprehensive about using the interface (23.8%). Despite careful attention to the legal rationale for access and an interface design that limits access to a worker's own caseload, 22.7% of survey respondents who used the KHIDS interface indicated that they felt nervous that they might access information they should not.

The Division of Analytics researchers who analyzed the survey results concluded that:

> Based on the results of the survey, it seems most workers are not utilizing the KHIDS function with the TWIST system, though opinions are generally favorable among workers who do utilize the system. Frequency of use remains low for many workers, and general confusion exists among reading and understanding the documentation available within the KHIDS interface. While most workers

understood the value of the KHIDS system, a general sense of apprehension surrounding the software remained among many workers.[19]

The survey results showed KHIDS program personnel and partners that CWWs needed additional training to make sure they knew how to navigate the interface and understand that the interface is meant to support them and make their jobs easier. It also showed program personnel and partners the potential value of further evaluation efforts, including repeating the survey with additional questions that focus on outcomes associated with interface use. In particular, they would like to assess whether an increased utilization of KHIDS improves the well-being of DCBS's foster children.

Lessons Learned and Recommendations

The KHIDS program personnel and partners interviewed for this case study identified lessons learned and recommendations from their work with the implementation and ongoing operations of the KHIDS interface. Interviewees provide the following information to others who would like to build a similar data sharing system or interface:

- Ensure that your privacy officer is involved right from the beginning. These systems involve the sharing of sensitive and confidential data. To protect the data from being accessed inappropriately, your privacy officer may require changes to your initial plans. Knowing from the start what your privacy officer will and will not allow will help you avoid the additional time and cost associated with making changes after work on the system has already begun.

- Engage all possible collaborators, contributors, and intended users at the start of a project to help facilitate project implementation. When interested parties are involved in a project from the beginning, they are more likely to understand the project and how the data will be used, which makes it easier to work with them to complete the necessary agreements and get the project off the ground. By comparison, if you start the project in a silo, then find you need to engage another party, they will be new to the project, and it may take additional time to acquire their support. A solution is to engage all parties with potential interest in the project from the beginning, even if there is a chance that party may not actually need to be involved.

- The training given to system users is an important part of the overall system implementation. All collaborators, including the privacy officer, should review training materials to ensure it will teach trainees about the system and how to use it.

- Include a robust evaluation piece in your project. Evaluating system utilization will let you know what users need (if anything) to make better use of the system. The lessons KHIDS program personnel learned by evaluating system utilization were helpful in

[19] Ibid, page 2.

improving the process. Eventually, the program hopes to assess whether increased system utilization improves the well-being of DCBS's foster children.

These lessons and recommendations highlight what those involved in KHIDS learned while implementing a data sharing initiative involving HIPAA protected healthcare records. The organization's CPO played an important role in ensuring a legally compliant design. The resulting interface provides a good example for others who would like to create a similar data sharing initiative.

Appendix A

KHIDS Memorandum of Understanding

Memorandum of Understanding (MOU)
Between
The Kentucky Department for Medicaid Services,
The Kentucky Department for Community Based Services,
and
The Kentucky Office of Data Analytics

This intra-agency Memorandum of Understanding ("MOU") is entered into by and between the Kentucky Department of Medicaid Services ("DMS"), the Kentucky Department for Community Based Services ("DCBS"), and the Kentucky Office of Data Analytics ("ODA"), Division of Health Information, ("DHI"); all agencies are organizational units within the Kentucky Cabinet for Health and Family Services.

WHEREAS, DMS is the single state Medicaid agency for the administration of medical assistance services in accordance with Title XIX of the Social Security Act and KRS 194A.030(2);

WHEREAS, DCBS is the state agency that provides services for dependent, neglected, and abused children, and their respective families, as well as children who are at imminent risk and in need of services to prevent entry into DCBS custody, as provided by KRS 194A.030(8);

WHEREAS, DHI, as a sub-unit of ODA, is the state agency responsible for providing leadership in the redesign of the health care delivery system using electronic information technology as a means to improve patient care and reduce medical errors and duplicative services, as provided under KRS 194A.030(7) and 194A.103, and in accordance with this authority operates the Kentucky Health Information Exchange ("KHIE");

WHEREAS, KHIE has developed a Participation Agreement ("PA") that lists the Permitted Purposes for which certain Participants may access, use, and disclose information contained within KHIE, and the Permitted Purposes for DMS include: for Treatment and Payment for Medicaid patients and/or Operations as these terms have been defined in the Permitted Use section (a) above such that patient authorization is not required under HIPAA, limited to functions related to case management, care coordination, and quality improvement activities; and any further references to "Participant" refer to DMS in its capacity as a KHIE Participant;

WHEREAS, Participant may designate "Authorized Users" to act on behalf of Participant to access KHIE information, limited to Participant's Permitted Purposes, and DMS desires to designate certain employees of DCBS as its Authorized Users, and Participant remains responsible for all system access of its Authorized Users;

WHEREAS, DMS desires for its DCBS Authorized Users to be allowed access to certain data that is confidential and must be afforded special protection, and DMS desires that DCBS Authorized Users shall receive and have access to data on behalf of DMS for purposes of care coordination which is only to be accessed, used, or disclosed in accordance with this Agreement and in accordance to state and federal law;

WHEREAS, Title IV-E of the Social Security Act (42 U.S.C. § 670 et seq.) requires the state child welfare agency (DCBS) to develop case plans for children in foster care, including the most recent information available regarding the child's health providers, immunization records, medications and any other

relevant health information as determined by the child welfare agency (42 U.S.C. §§ 671(a)(16), 675(1)(C);

WHEREAS, 45 CFR 164.502(g) mandates that when state law allows a minor patient to consent to his or her own treatment without requiring consent from the minor's guardian/personal representative, such records may not be accessed by the minor's guardian/personal representative. KRS 214.185 allows a minor patient to consent to certain types of treatment, and as such it is understood that records included under KRS 214.185 will be excluded from the records a DCBS Authorized User is allowed to access;

WHEREAS, DMS and DCBS have a common interest in assuring that their eligible enrollees and clients gain access to medical services and attain or maintain favorable physical and mental health by securing services and in fulfilling the federal and state requirements of both agencies; and

WHEREAS, DMS, DCBS, and DHI mutually recognize that coordination between the agencies will serve the best interest of the citizens of Kentucky;

NOW, THEREFORE, DMS, DCBS, and DHI agree as follows:

Purpose of MOU: The Fostering Connections to Success and Increasing Adoptions Act of 2008 (PL 110-351) requires State Title IV-B agencies to develop a plan for oversight and coordination for health care services for children In foster care, in coordination and consultation with the State Title XIX Medicaid agency. This requirement aims to ensure that children in foster care receive high-quality, coordinated health care services, including appropriate oversight of prescription medication (sect. 422(b)(15)). DCBS serves as Kentucky's state Title IV-B agency and is the caregiver/custodian of children in the agency's custody. DCBS is required to participate in the medical management of children in the agency's custody and to conduct oversight for health services.

This MOU will allow DMS to share provider records from KHIE with DCBS Authorized Users to improve coordination of care for children in the custody of DCBS and help ensure that services are delivered in a timely, appropriate, efficient, and cost-effective manner.

DMS will allow certain data from KHIE to be accessed by its DCBS Authorized Users on behalf of DMS in order to assist in the coordination of medical and health care services for children enrolled in Medicaid who are also in the care and custody of DCBS only if permitted by state and federal law, and in accordance with 42 C.F.R. § 431.300-307.

DMS agrees to allow for its DCBS Authorized Users to obtain and use only information from Provider records for Medicaid-enrolled individuals who are in the custody of DCBS, and only those records as allowed under law and this Agreement.

Point of Contact (POC) Responsibility: DCBS and DMS designate the following individuals as their agency Point of Contact (POC) for any data received from the other agency; those individuals will agree to the responsibilities as outlined below:

Agency	Department of Community Based Services POC for DMS Data	Department of Medicaid Services POC for DCBS Data
Contact Name		
Street Address		
City/State/ZIP Code		
Telephone Number		
E-mail Address		

The Point of Contact shall be responsible for the observance of all conditions of use and for the establishment and maintenance of safeguards to prevent unauthorized use. Either party shall notify the other party in writing within ten (10) calendar days of any change of the designated POC. Notification of change of the POC shall be delivered by an acceptable method agreed upon by the parties, such as certified mail, return receipt requested, or in person with proof of delivery, or via email.

Permissible Uses and Disclosures of Data: DCBS shall not use or further disclose, transmit, copy, or disseminate the data specified in this MOU except as permitted by this MOU or as required by federal law.

DCBS shall establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of and to prevent unauthorized use or access to the data specified in this MOU.

DCBS shall ensure that all electronic transmissions of protected health information are authorized by the terms of this MOU and that all transmissions shall be protected from improper disclosure. DCBS shall use appropriate authentication and encryption systems to safeguard all protected health information from improper disclosures.

DCBS shall restrict disclosure of the data specified in this MOU to the minimum number of individuals who require the information in order to perform the functions of this MOU. DCBS shall instruct individuals to whom the data is disclosed of all obligations under this MOU and shall require the individuals to maintain those obligations, and shall maintain documentation of each individual's agreement to do so.

DCBS shall secure the data specified in this MOU when the data is not under the direct and immediate control of an authorized individual performing the functions of this MOU. DCBS shall make a good faith effort to identify any use or disclosure of the data not provided for by this MOU. DCBS shall notify DMS and the Cabinet's Privacy Officer by agreed upon methods such as electronic mail, phone, or certified mail, return receipt requested, or in person with any proof of delivery within forty-eight (48) hours of discovery of any use or disclosure of the data not provided for by this MOU of which DCBS is aware. Contact information for those individuals is included near the end of this Agreement.

DCBS shall not release or allow the release of the data specified in this MOU to any person or entities other than as permitted by this MOU.

A violation of this section shall constitute a material breach of this MOU.

Required Activities: DCBS will identify children in DCBS custody and will provide DMS and KHIE with a daily updated list of those children, including notification of when a child is no longer in DCBS custody.

This is in order to create an accurate patient panel of only those individuals whose records the Authorized User is allowed to access. KHIE will match files to identify children receiving Medicaid benefits and provide access to medical and pharmacy clinical and claims information for those beneficiaries in DCBS custody. DCBS Authorized Users will access the patient panel via the TWIST platform.

DCBS Authorized Users shall ONLY be allowed to access records for children in the custody of the Cabinet who are currently in the Authorized User's caseload and matched to the Authorized User's patient panel. Patient information may only be viewed upon entry into DCBS custody, and Authorized Users must cease viewing information when the child is no longer in DCBS custody. DCBS Authorized Users shall only access the records for those individual children who are listed in the Authorized User's patient panel, with a very limited exception addressed below.

In the event that a child who is in DCBS custody does not appear on an Authorized User's patient panel, the Authorized User must initiate the process to request to search for that patient's records within KHIE. In order to view records of a patient who is not listed on the Authorized User's patient panel, the Authorized User must confirm and attest that he or she is authorized to view that record, under penalty of law. This acknowledgement shall be retained electronically and a daily report of any such access will be sent to an Access Administrator who has been authorized to review the report. The Access Administrator shall verify access by all Authorized Users for any record that is accessed outside of the Authorized User's patient panel to ensure the need for the Authorized User to access that record. The Access Administrator shall immediately notify and report any unauthorized access of records to KHIE and DMS.

KHIE will send an "event notification" to Authorized Users when an "event" occurs in the KHIE record of a child who has been matched to the Authorized User's patient panel. The definition of an "event" shall be determined by KHIE and is subject to change based on KHIE standards, policies, and procedures.

DMS, as a KHIE Participant shall designate an individual who will be authorized to assign and approve user credentials to Authorized Users within the Participant's workforce. This individual will also serve as a contact person to receive communication from KHIE. DMS, as the Participant, will be responsible for all of its Authorized User's use of the KHIE system.

The Parties shall require that all of Participant's Authorized Users will access and use KHIE only in accordance with the terms and conditions of this Agreement and DMS' Agreement with KHIE.

The Parties shall discipline appropriately any of their employees or Authorized Users who fail to act in accordance with the terms and conditions of this Agreement relating to the privacy and security of Message Content, in accordance with the Parties' employee disciplinary policies and procedures.

DCBS shall provide appropriate training to Authorized Users before they first receive access to KHIE, and at least annually thereafter. The content of this training must be agreed upon and approved by all parties as well as the CHFS Chief Information Security Officer and Chief Privacy Officer.

Authentication: DMS shall employ a process by which DMS, or its designee, uses the credentials issued to Authorized Users to verify the identity of each Authorized User prior to enabling such Authorized

User to access KHIE's system. This process shall include the completion of KHIE's Onboarding process by DMS before assigning user credentials.

DMS shall only assign user credentials to Authorized Users who are workforce members or agents of Participant. In the event of changes in the employment status of an Authorized User, DMS or other authorized personnel shall change the access or level thereof of the Authorized User within five (5) business days of the employment change.

Security: All parties agree to abide by the security requirements as outlined in DMS' Agreement with KHIE.

Term Agreement: This Agreement shall be effective beginning upon signature and continue through December 31, 2022 unless terminated pursuant to the termination clause contained herein. This Agreement may be extended for another term of two (2) years by mutual agreement of the parties in writing prior to December 31, 2022. Notwithstanding any of the foregoing, either party may terminate and cancel this Agreement, upon thirty (30) days written notice served on the other party outlining the reasons for cancellation or immediately for cause.

Upon termination of this Agreement, each party agrees to delete or destroy all information, records, data, reports, or derived products provided by the other party unless authorization to maintain the information is provided or required by law.

Notice to Agencies: Any notice required under this Agreement, including notice in the event of a potential breach, shall be made to the following contacts:

Department for Medicaid Services
Cabinet for Health and Family Services
275 East Main Street
Frankfort, Kentucky 40621
Attention: DMS Privacy Officer
Phone:
Email address:

Department for Community Based Services
Cabinet for Health and Family Services
275 East Main Street
Frankfort, Kentucky 40621
Attention: DCBS Privacy Officer
Phone:
Email address:

Division of Health Information (KHIE)
Cabinet for Health and Family Services
275 East Main Street
Frankfort, Kentucky 40621
Attention: KHIE Administrator, ODA
Phone:
Email address:

Chief Privacy Officer
Cabinet for Health and Family Services
275 East Main Street
Frankfort, Kentucky 40621
Attention: Chief Privacy Officer, ODA
Phone:
Fax:
Email address:

ORIGINAL AGREEMENT

Approvals

This Memorandum of Understanding (MOU) is subject to the terms and conditions stated herein. By affixing signatures below, the parties verify that they are authorized to enter into this agreement and that they accept and consent to be bound by the terms and conditions stated herein. In addition, the parties agree that (i) electronic approvals may serve as electronic signatures, and (ii) this agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all counterparts together shall constitute a single agreement.

CHFS Signature:

Signature Title

Printed Name Date

DMS Signature:

Signature Title

Printed Name Date

DCBS Signature:

Signature Title

Printed Name Date

ODA Signature:

Signature Title

Printed Name Date

Security Signature:

Signature Title

Printed Name Date

Approved as to form and legality:

Signature Date

Legal:

Signature Date

Appendix B

Business Associate Agreement between DMS, DCBS, and KHIE

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) is entered into as of the date listed in the Memorandum of Understanding by and between the Covered Entity listed in the Service Contract ("Covered Entity" hereinafter), whose principal place of business is located at listed in the Memorandum of Understanding and the Business Associate listed in the Memorandum of Understanding ("Business Associate" hereinafter), whose principal place of business is located at the address listed in the Memorandum of Understanding, in conformance with the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations ("HIPAA RULES" hereinafter).

RECITALS

Whereas, the Covered Entity has engaged the services of the Business Associate for or on behalf of the Covered Entity in Memorandum of Understanding # M957;

Whereas, the Covered Entity must disclose individually identifiable health information to the Business Associate in the performance of services, referenced in the Service Contract, for or on behalf of the Covered Entity;

Whereas, such information is Protected Health Information (PHI) as defined by the Privacy, Security, and Breach Notification and Enforcement Rules promulgated under HIPAA;

Whereas, the Parties agree to establish safeguards for the protection of such information;

Whereas, the Covered Entity and Business Associate desire to enter into this Agreement to address certain requirements under the HIPAA Rules as required by the implementing regulations;

Now Therefore, the parties hereby agree as follows:

SECTION I – DEFINITIONS

Relevant terms used in this Agreement shall have the same meaning as those terms found in the HIPAA rules found at 45 CFR §164.402; 45 CFR § 164.501; §164.304; and §160.103. The following terms, as defined in the HIPAA implementing regulations and used herein, shall mean:

1.1 "Breach" is defined as any unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI, unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based upon a risk assessment as required under 45 CFR § 164.402. The definition of Breach excludes the following uses and disclosures:

a. Unintentional acquisition, access or use of protected health information by a workforce member or person acting under the authority of a Covered Entity or Business Associate, if performed in good faith and within the scope of authority, and does not result in further unauthorized disclosures;

b. Inadvertent one-time disclosure between Covered Entity or Business Associate work force member to another work force member at the same covered entity or Business Associate who is authorized to access PHI and information received or disclosed is not further used or disclosed in a manner not permitted under Subpart E found at 45 CFR § 164.500, et seq.; and

c. The Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information.

1.2 "Business Associate" shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR §160.103, and includes a person or entity who creates, receives, maintains, or transmits PHI for a function or activity of the covered entity as set out under the regulation, and includes any subcontractor of the business associate who creates, receives, maintains, or transmits PHI on behalf of the business associate under 45 CFR § 160.103 (3) (iii).

1.3 "Covered Entity" shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR §160.103.

1.4 "Data Aggregation" shall have the meaning given to such term under the HIPAA Rules, including but not limited to, 45 CFR §164.501.

1.5 "Designated Record Set" shall have the meaning given to such term under the HIPAA Rules, including, but not limited to 45 CFR §164.501.

1.6 "Effective Date" shall be the Effective Date of this amended and restated Agreement.

1.7 "Electronic Protected Health Information" or "Electronic PHI" shall have the meaning given to such term at 45 CFR §160.103, limited to information of the Covered Entity that the Business Associate creates, receives, maintains or transmits in electronic media on behalf of the Covered Entity under the terms and conditions of this Agreement.

1.8 "Health Care Operations" shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR §164.501.

1.9 "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules codified at 45 CFR Part 160 and Part 164.

1.10 "Individual" shall have the meaning given to such term in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

1.11 "Individually Identifiable Health Information" shall have the meaning given to such term under the HIPAA Rules, including, but not limited to 45 CFR §160.103.

1.12 "Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an Individual; the provision of health care to an Individual; or the past, present or future payment for the provision of health care to an Individual; and (ii) that identifies the Individual or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual, and shall have the meaning given to such term in 45 CFR §160.103, limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

1.13 "Required by Law" shall have the meaning given to such phrase in 45 CFR §164.103.

1.14 "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

1.15 "Security Incident" shall have the meaning given to such phrase in 45 CFR §164.304.

1.16 "Unsecured Protected Health Information" shall mean protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary. (45 CFR §164.402), except that Unsecured Protected Health Information shall be limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

SECTION II – OBLIGATIONS AND ACTIVITIES OF THE BUSINESS ASSOCIATE

The Business Associate agrees to the following:

2.1 Not to use or further disclose PHI other than as permitted or required by this Agreement and to fulfill its responsibilities under the contract setting out the scope of work for the Business Associate, or as required by law, or for the proper management and administration of the business associate under the requirements set out in Section III below;

2.2 To use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement;

2.3 To mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of this Agreement or the HIPAA Privacy and Security Rules;

2.4 To report to the Covered Entity any use or disclosure involving PHI not provided for by this Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR § 164.410, and any Security Incident of which it becomes aware. The business associate shall immediately report to the covered entity any breach of unsecured PHI, except as provided by 45 CFR § 164.412 based upon a request from law enforcement to delay the notice in that such would impede a criminal investigation or cause damage to national security. The Business Associate shall provide to the covered entity the following information: (1) a brief description of what happened; including the date of the breach and date of discovery of the breach, if known; (2) identification of each individual whose unsecured PHI has been affected by the breach; (3) description of the type of unsecured PHI involving the breach; (4) any steps the individuals should take to protect themselves from harm from the breach; and (5) steps the Business Associate is taking to investigate the breach, to mitigate harm and protect against other breaches. The Business Associate, in consultation with the covered entity, shall be responsible for breach notifications to individuals affected by the unauthorized use or disclosure no later than sixty (60) days following its discovery or by exercise of reasonable due diligence would have been known to the Business Associate, as required by 45 CFR § 164.404. The Business Associate shall be solely responsible for any and all costs associated with the notification requirements to the individuals as provided herein. The Business Associate shall be responsible for any penalties, assessments or fees assessed by the Office for Civil Rights/Department of Health & Human Services due to any breach caused by the Business Associate or based upon the failure of the Business Associate to comply with the HIPAA Privacy and Security Rules. The covered entity, in consultation with the Business Associate, shall make all needed notices to the media and the Secretary of HHS. The Business Associate shall report immediately to the covered entity any security incident of which it becomes aware as required by 45 CFR § 164.314 (a) (2) (i) (C). The Business Associate shall report to the covered entity the operative facts surrounding the security incident, what steps are to be taken to address the security incident, and other information which may be requested by the covered entity relative to the security incident.

2.5 In accordance with 45 CFR §§164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any agent, including a subcontractor, that creates, receives, maintains, or transmits PHI on behalf of the Business Associate agrees in writing to the same restrictions, conditions and requirements that apply to the Business Associate with respect to such PHI;

2.6 To provide access to PHI in a Designated Record Set, at the request of the Covered Entity, and in the time and manner designated by the Covered Entity, to the Covered Entity, or as directed by the Covered Entity, to the Individual or the Individual's designee as necessary to meet the Covered Entity's obligations under 45 CFR §164.524; provided, however, that this Section 2.6 is applicable only to the extent the Designated Record Set is maintained by the Business Associate for the Covered Entity;

2.7 To make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR §164.526 at the request of the Covered Entity or an Individual, and in the time and manner designated by the Covered Entity; provided, however, that this Section 2.7 is applicable only to the extent the Designated Record Set is maintained by the Business Associate for the Covered Entity;

2.8 To make internal practices, books and records, including policies and procedures on PHI, relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, the Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary's determining the Covered Entity's and the Business Associate's compliance with the HIPAA Rules;

2.9 To document non-routine disclosures of PHI and information related to such disclosures 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 CFR §164.528, where applicable;

2.10 To provide to the Covered Entity or an Individual, in a time and manner designated by the Covered Entity, information collected in accordance with Section 2.9 of this Agreement, to permit the Covered Entity to respond to a request by an accounting of disclosures of PHI in accordance with 45 CFR §164.528;

2.11 That if it creates, receives, maintains, or transmits any electronic PHI (other than enrollment/disenrollment information and Summary Health Information, which are not subject to these restrictions) on behalf of the covered entity, it will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information, and it will ensure that any agents (including subcontractors) to whom it provides such electronic PHI agrees to implement reasonable and appropriate security measures to protect the information;

2.12 Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent the use or disclosure of protected health other than is permitted for under this Agreement or required by law;

2.13 To retain records related to the PHI hereunder for a period of six (6) years unless the Agreement is terminated prior thereto. In the event of termination of this Agreement, the provisions of Section V of this Agreement shall govern record retention, return or destruction;

2.14 Implement administrative safeguards in accordance with 45 CFR §164.308, physical safeguards in accordance with 45 CFR §164.310, technical safeguards in accordance with 45 CFR §164.312, and policies and procedures in accordance with 45 CFR §164.316;

2.15 Shall appropriately safeguard any and all PHI provided by the covered entity to the Business Associate under the service contract or agreement as required under HIPAA Rules and this Agreement herein, as set out in 45 CFR §164.502 (e) (1) and (2).

2.16 Not to make any fundraising communication on behalf of Covered Entity or to Covered Entity's participants and beneficiaries;

2.16 Not to receive any remuneration, either directly or indirectly, in exchange for PHI, except as may be permitted by 45 CFR §164.502(a)(5) and §164.508(a)(4);

2.17 Not to make any marketing communication on behalf of Covered Entity or to Covered Entity's participants and beneficiaries, except as may be permitted by 45 CFR §164.501; and

2.18 To the extent Business Associate is to carry out one or more of the Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligations.

SECTION III – THE PARTIES AGREE TO THE FOLLOWING PERMITTED USES AND DISCLOSURES BY THE BUSINESS ASSOCIATE

3.1 Business Associate agrees to make uses and disclosures and requests for PHI consistent with the Covered Entity's minimum necessary policies and procedures.

3.2 Except as otherwise limited in this Agreement, the Business Associate may use or disclose PHI to perform functions, activities or services for, or on behalf of, the Covered Entity as specified in the Agreement, provided that such use or disclosure would not violate the HIPAA Rules if done by the Covered Entity; and

3.3 Except as otherwise limited in this Agreement, the Business Associate may:

a. Use for management and administration. Use PHI for the proper management and administration by the Business Associate or to carry out the legal responsibilities of the Business Associate; and,

b. Disclose for management and administration. Disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are Required by Law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

SECTION IV – NOTICE OF PRIVACY PRACTICES

4.1 The Covered Entity shall (a) provide the Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 CFR §164.520, as well as any changes to such notice; (b)

provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures; (c) notify the Business Associate of any restriction to the use or disclosure of PHI that the Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restrictions may affect the Business Associate's use or disclosure of PHI; and (d) refrain from requesting the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by the Covered Entity, except as provided herein.

SECTION V – BREACH NOTIFICATION REQUIREMENTS

5.1 With respect to any Breach by the Business Associate as provided in Section 2.4 above, the Business Associate shall notify each individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, used, or disclosed as a result of such Breach, except when law enforcement requires a delay pursuant to 45 CFR §164.412:

a. Without unreasonable delay and in no case later than sixty (60) days after discovery of a Breach or from the time it should have reasonable been discovered;

b. By notice in plain language including and to the extent possible:

1) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

2) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3) Any steps individuals should take to protect themselves from potential harm resulting from the Breach;

4) A brief description of what the Covered Entity involved is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and,

5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

c. Use a method of notification that meets the requirements of 45 CFR §164.404(d); and

d. The Business Associate shall provide for substitute notice, as required by HIPPAA Rules, by providing a toll-free phone number that remains active for at least ninety (90) days where an individual can learn whether the individual's unsecured PHI may be included in the breach and a posting as required by 45 CFR § 164.404 (d)(2). The costs of the substituted notice and notifications set out in this Section shall be the responsibility of the Business Associate.

SECTION VI – TERM AND TERMINATION

6.1 Term. The term of this Agreement shall be effective as of the date set forth above in the first paragraph and shall terminate when all of the PHI provided by the Covered Entity to the Business Associate, or created or

received by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, 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.

6.2 Termination for Cause. Upon the Covered Entity becoming aware of a material breach of this Agreement by the Business Associate, the Covered Entity shall provide an opportunity for the Business Associate to cure the breach or end the violation. The Covered Entity shall terminate this Agreement and the Service Contract if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity, or terminate this Agreement immediately if a cure is not possible.

If the Business Associate fails to cure a breach for which cure is reasonably possible, the Covered Entity may take action to cure the breach, including but not limited to obtaining an injunction that will prevent further improper use or disclosure of PHI. Should such action be taken, the Business Associate agrees to indemnify the Covered Entity for any costs, including court costs and attorneys' fees, associated with curing the breach.

Upon the Business Associate becoming aware of a material breach of this Agreement by the Covered Entity, the Business Associate shall provide an opportunity for the Covered Entity to cure the breach or end the violation. The Business Associate shall terminate this Agreement if the Covered Entity does not cure the breach or end the violation within the time specified by the Business Associate, or terminate this Agreement immediately if the Covered Entity has breached a material term of this Agreement if cure is not possible.

6.3 Effect of Termination.

a. Return or Destruction of PHI. Except as provided in Section 6.3(b), upon termination of this Business Agreement, for any reason, the Business Associate shall return, or if agreed to by the Covered Entity, destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of PHI.

b. Return or Destruction of PHI Infeasible. In the event that the Business Associate determines that returning or destroying PHI is infeasible, the Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction not feasible. Upon mutual agreement of the parties that return or destruction of the PHI is infeasible, the Business Associate shall extend the protections of this Agreement 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 the Business Associate maintains such PHI. In addition, the Business Associate shall continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 to prevent use or disclosure of the PHI, for as long as the Business Associate retains the PHI.

SECTION VII – GENERAL PROVISIONS

7.1 Regulatory References. A reference in this Agreement to the HIPAA Rules or a section in the HIPAA Rules means that Rule or Section as in effect or as amended from time to time.

7.2 Compliance with Law. In connection with its performance under this Agreement, Business Associate shall comply with all applicable laws, including but not limited to laws protecting the privacy personal information about individuals.

7.3 Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the Parties to comply with the HIPAA Rules and any other applicable law. This Agreement may not be modified, nor shall any provision herein be waived or amended, except in a writing duly signed by the authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

7.4 Confidentiality Obligations. In the course of performing under this Agreement, each Party may receive, be exposed to or acquire "Confidential Information," including but not limited to, all information, data, reports, summaries, tables and studies, whether written or oral, fixed in hard copy or contained in a computer data base or computer readable form, as well as any information identified as "Confidential Information" of the other Party. For purposes of this Agreement "Confidential Information" shall not apply to PHI, the privacy and security of which is the subject of this Agreement and addressed throughout the terms herein. The parties including their employees, agents and representatives shall: (a) not disclose to any third-party "Confidential Information" of the other party except as permitted under this Agreement; (b) only permit use of "Confidential Information" of employees, agents or representatives having a need to know in connection with performance under this Agreement, and (c) advise each of its employees, agents and representatives of their obligations to keep such "Confidential Information" confidential. This provision shall not apply to "Confidential Information": (i) after it becomes publicly available through no fault of either party; (ii) which is later publicly released, in writing, by the party that owned the material; (iii) which is lawfully obtained by the third parties without restriction; or (iv) which can be shown to be previously known or developed by either party independently of the other party.

7.5 No Third-Party Beneficiary. The parties do not express or imply by any terms in this Agreement to confer any rights, remedies or entitlements upon any third person not a party to this Agreement herein. The parties agree that there are no third-party beneficiaries intended to be benefited by this Agreement.

7.6 Indemnification by Business Associate. Business Associate agrees to indemnify, defend and hold harmless the Covered Entity and its employees, directors, officers, subcontractors, agents or other members of its workforce, each of the foregoing hereinafter referred to as "Indemnified Party," against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with Business Associate's actions arising out of this Agreement. Accordingly, on demand, Business Associate shall reimburse any Indemnified Party for any and all actual and direct losses, liabilities, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any Indemnified Party by reason of any suit, claim, action, proceeding or demand by any third party which results for Business Associate's breach hereunder. The obligation to indemnify any Indemnified Party shall survive the expiration or termination of this Agreement for any reason.

7.7 Survival. The respective rights and obligations of Business Associate under Section II and Section 6.3(b) of this Agreement shall survive the termination of this Agreement.

7.8 Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the HIPAA Rules.

7.9 Notices. Notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address listed in the Service Contract, and/or (other than for delivery fees) via facsimile to the facsimile telephone numbers listed in the Service Contract:

Each party named in the Service Contract may change update its address and that of its representative for notice by giving notice thereof in the manner herein provided.

7.10 Counterparts: Facsimiles. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

7.11 Disputes. If any controversy, dispute or claim arises between the Parties with respect to his Agreement, the parties shall make good faith efforts to resolve such matters informally. Any dispute that cannot be mutually settled may be brought in the Franklin Circuit Court or Federal District Court of Kentucky.

7.12 Mutual Representations and Warranties. Each party represents and warrants to the other party that is duly organized and validly existing, and in good standing under the laws of the jurisdiction under which it is organized or licensed, it has the full power to enter into this Agreement and to perform the obligations hereunder, and that the performance of it of its obligations under this Agreement have been duly authorized by all necessary corporate or other actions and will not violate any provisions of any license, corporate charter or bylaws.

In Witness Wherefore, the Parties hereto acknowledge agreement with the terms herein and have duly executed this Agreement as of the Effective Date as defined here above by setting forth their signatures below.

Covered Entity	**Business Associate**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date: