INTERGOVERNMENTAL AGREEMENT FOR INFORMATION SHARING

This multi-party intergovernmental agreement (this "Agreement") is entered into as of September 1, 2020, by and among the City of St. Louis Criminal Justice Coordinating Council ("CJCC") and each of its member agencies (each a "CJCC Member"). The CJCC and each CJCC Member a "Party," and collectively the "Parties").

WHEREAS, the City of St. Louis Criminal Justice Coordinating Council is an independent advisory council that makes recommendations to those elected and appointed officials who have the authority to implement such recommendations, as they deem appropriate; and

WHEREAS, the City of St. Louis Board of Aldermen established the CJCC by passing Ordinance 71012 (the "Ordinance") on July 12, 2019, which was signed by the Mayor and became effective on August 26, 2019;

WHEREAS, the CJCC Members have entered into an Intergovernmental Cooperative Agreement (the "ICA") which governs the formation, organization, and corporate governance of the CJCC;

WHEREAS, the purpose of the CJCC is to "ensure the fair administration of criminal and juvenile justice by increasing effective communication, collaboration and planning; and, to improve the criminal and juvenile justice systems' operation through effective data collection, sharing and analysis crosscutting the local criminal and public health system"; and

WHEREAS, the Ordinance requires that the CJCC will maintain an intergovernmental information sharing agreement among the Parties and other public and private entities to implement and govern the sharing of information among them in lawful, secure, effective, simple, and practical manner, and this Agreement satisfies such requirement; and

WHEREAS, the CJCC Members wish to establish a trusted information sharing environment in which their mutual interests are protected and their expectations and requirements are clearly documented in furtherance of their intent to share data and information in furtherance of the CJCC's stated purpose with departments, divisions, portions of Member agencies and the public to the greatest extent permitted by law, while protecting personal and other confidential information in compliance with applicable law, in order to better serve the public and to improve operations across and among CJCC Members; and

WHEREAS, the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) provides federal regulations, as administered by the CJIS Systems Agency (CSA) designated by the FBI (currently Missouri Highway Patrol (MSHP)) on appropriate use and dissemination of Criminal Justice Information (CJI); and

WHEREAS, the CJIS Security Policy is an existing, reliable, and well-understood regulatory framework applicable to the use of certain CJI, and the CJCC adopts this same framework when sharing information internally or externally to other parties; and,

WHEREAS, it is the intent of the CJCC that criminal justice agencies continue to follow the CJIS Security Policy when required; and

WHEREAS, the CJCC commits to the following state and federal requirements:

- Mo. Rev. Stat. § 610.010 et. seq, and the Missouri Sunshine Law provide regulations governing the inspection and release of records; and

- Missouri crime victims rights laws, including Article 1, Section 32 of the Missouri Constitution and Mo. Rev. Stat. §595.209; and

- Title 42, Code of Federal Regulations, Part 2, which provides federal regulations governing the confidentiality and disclosure of Alcohol and Drug Abuse Patient Records for individuals receiving substance abuse treatment; and

- The Health Insurance Portability and Accountability Act ("HIPAA"), Title 45, Code of Federal Regulations Parts 160, General Administrative Requirements, 162, Administrative Requirements and 164, Security and Privacy, which establish regulations governing the confidentiality and disclosure of Protected Health Information, including that the release of psychotherapy notes must be requested on a separate form from any other health information; and

- 28 C.F.R. Part 20 and 28 U.S.C. § 534, which provide regulations relating to the collection, use, dissemination, and control of Criminal History Record Information (CHRI); and

WHEREAS, it is the intent of this Agreement to provide the framework to guide and regulate the definition, design, development, implementation, use and support of all information exchanges under the purview of the CJCC through the execution of separate and subsequent agreements between the parties involved in the information exchange.

The following index of defined terms and acronyms reflects the section in which the definition of such terms and acronyms can be found:

Defined Term	**Section**
Agreement	Preamble
business associate	Exhibit A
CHRI	Recitals
CJCC	Preamble
CJCC Member	Preamble
CJI	Recitals
CJIS	Recitals
CJIS Policy	2.2
CSA	Recitals
FBI	Recitals
HIE	Exhibit A
HIPAA	Recitals

Defined Term	**Section**
ICA	Recitals
ISGC	1.2
ISOs	1.3
MSHP	Recitals
Ordinance	Recitals
ORI	2.2.4
Party or Parties	Preamble
QSOA	Exhibit A

AGREEMENT

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

ARTICLE I. CJCC RESPONSIBILITIES

1.1 The CJCC. The CJCC is responsible for establishing and implementing policies for the sharing of criminal justice information among the CJCC Members. Each of the CJCC Members agrees to comply with such policies that are adopted by the CJCC in accordance with the ICA and the CJCC bylaws.

1.2 The ISGC. The Information Sharing Governance Committee ("ISGC"), a committee of the CJCC, will have the principal responsibility to review and make recommendations to the CJCC regarding the sharing of information among CJCC Members.

1.3 The CJCC Executive Director. The CJCC Executive Director, as an agent for and under the direction of the CJCC, is responsible for the promulgation and implementation of the CJCC policies relating to the sharing of CJI among CJCC Members, the auditing and implementation of those policies, and the facilitation of the creation and maintenance of an information security organization comprised of Information Security Officers ("ISOs") from each CJCC Member.

1.4 Information Governance. The ISGC will define governance and security features that will limit the availability of CJI to certain CJCC Members, or in some cases, certain representatives of a CJCC Member, and third party entities depending upon the role of the CJCC Member or entity, and the type of CJI. The CJCC Executive Director will be responsible for implementing such governance and security features, under the direction of the CJCC, and granting permission to access CJI based on the required needs and privileges of the request.

1.5 CJCC Services. The CJCC may develop data analysis services and capabilities, which may include:

1.5.1. *Dashboards and portals* – Dashboards represent predefined data analyses that are typically presented in graphical form on a webpage and referred to as "visualizations". Multiple visualizations can be presented on the webpage reflecting data analyses of interest to the audience. Each component can provide limited filtering, such as a count of crimes by offense type or by date. This is the simplest tool to use and is intended for the broadest, least technically sophisticated audience. It would be used for a public-facing dashboard, for example. Development of these capabilities should be relatively low cost to develop and maintain. SEARCH has an example of this at http://demo.ojbc.org/dashboards/jail-booking-dashboard.html.

1.5.2. *Business Intelligence Tools* – These tools provide users with a more robust set of analytic capabilities, yet do not require special technical expertise to use. These tools give users who are familiar with the data they want to work with the capability to create unique queries to answer broader research and policy questions. Such tools provide a "workbench" user interface that allows the user to drag and drop various types of data to produce tables and graphics. These

tools provide all of the capabilities that are available to the user. There can be some limitations in how these tools can filter and aggregate data because all data is predefined within the tool in datasets commonly called "cubes". These tools are targeted at "super users" who know their data and are not intimidated by using a new software tool. The primary advantage and limitation of these tools is that the user does not have direct access to the data. Data is "curated" (cleaned and structured) "under the hood" by a data scientist to ensure that data are used in a consistent manner. In St. Louis, this tool is intended to be used by agency personnel responsible for analyzing data but are not necessarily trained as researchers, statisticians or data scientists. The BI Tool planned for use in St. Louis will be open source and free for use by authorized users. SEARCH has an example of this at http://demo.ojbc.org/saiku-ui/. A video demonstration of how to use this tool is located at https://www.youtube.com/watch?v=2aX1s6lNoAc&feature=youtu.be.

1.5.3. *Data Science/Analysis Tools* – These tools provide the most sophisticated data analysis capabilities. A variety of commercial data analysis tools are available to researchers, statisticians and data scientists (Tableau, STATA, SAS, etc.) as well as data science programming languages such as R and Python. These tools provide the user with total control over access to and use of data. They require the user to define the data to be used and how it will be used, curate or clean and standardize the data as well as define the specific queries to be performed. Many of these tools provide highly sophisticated analytic capabilities that go well beyond the data analysis capabilities provided in the BI Tools discussed above. These tools provide "the complete package" of data analysis and presentation capabilities. Many provide a user interface that is similar to the BI Tools discussed above. These are commercial products that require some form of licensing and on-going costs. The intent is to allow authorized users to receive de-identified datasets for use in these products.

ARTICLE II.CJCC MEMBER RESPONSIBILITIES

2.1 Information Security. Each CJCC Member will be responsible under specific legislative, regulatory and executive mandates to provide information to other persons only in certain circumstances and with certain specific safeguards, as permitted and required under such mandates. Without limiting the foregoing, Exhibit A summarizes information exchange requirements under the CJIS Policy, HIPAA, and Title 42 CFR Part 2.

2.2 CJIS Security Policy. Each CJCC Member is responsible for its own compliance with the Criminal Justice Information Services Security Policy published by the U.S. Department of Justice, Federal Bureau of Investigation (the "CJIS Policy") and the activities to be performed by such CJCC Member in accordance with CJIS Policy. Without limiting the foregoing, each CJCC Member agrees as follows:

2.2.1. Each CJCC Member has executed, or will execute, appropriate information exchange agreements with third parties, including those agreements required by the CSA to implement the CJIS Policy. Those agreements include an Information Exchange Agreement template for the exchange of information between two criminal justice agencies, and a Management Control Agreement template for the exchange of information between a criminal justice agency and a contracted non-criminal justice entity. To properly implement the CJIS Policy, these agreements must be substantially in the form provided by the CSA, and may only

be modified upon approval of all parties to the applicable agreement and the CSA. Copies of the CSA information exchange agreements are attached to Exhibit A.

2.2.2. Each CJCC Member will perform security awareness training as required by the CJIS Policy. The CJCC Members may elect to comply with such obligation by participating in MSHP training.

2.2.3. Each CJCC Member will implement appropriate audit and accountability controls with respect to their information systems that follow CJIS Policy standards.

2.2.4. Each CJCC Member will use its FBI authorized originating agency identifier (ORI) on each CJI transaction, Each agency that holds an ORI will have the responsibility to confirm compliance with the CJIS Policy with respect to its own information, including the requirement to enter into appropriate information exchange agreements with third parties. Organizations that do not have an ORI are not criminal justice agencies but can still receive CJI under certain conditions with the proper agreement in place.

2.2.5. CJCC Members may delegate one or more of the activities required by the CJIS Policy, but any delegate of such activities must comply with the CJIS Policy, and each CJCC Member will remain responsible for such compliance. The CJCC may establish acceptable mechanisms for the delegation of certain activities required by the CJIS Policy.

2.3 Acknowledgements. The CJCC acknowledges that each CJCC Member's primary responsibility with respect to information shared under this Agreement is to collect, assemble, share and analyze information in the course of providing services to its users and fulfilling its own mission and purpose. The processing, transmission, storage, or sharing of CJI between or among CJCC Members for any such purpose does not render such CJI public information. The CJCC Member that provides the information remains the owner of the CJI and is responsible for responding to Sunshine Law requests regarding all such information. The receiving Party has no obligation and no authority to respond to a Sunshine Law request on behalf of the providing Party.

ARTICLE III. LIABILITY

3.1 Each Party is responsible for its own conduct and the conduct of its employees, agents, and other users of shared information, and retains all defenses and immunities available under federal and Missouri laws. No Party will be obligated under this Agreement to insure, defend, or indemnify any other Party.

3.2 Each CJCC Member may be audited for compliance with this Agreement by the CJCC in accordance with policies and procedures as may be established by the CJCC and will be subject to any remedies for noncompliance as set forth in such policies.

ARTICLE IV. DISPUTE RESOLUTION

In the event of a dispute, the Parties agree to use their best efforts to resolve the dispute in an informal fashion through consultation and communication, or other forms of nonbinding alternative dispute resolution mutually acceptable to them. As necessary, the Parties will pursue

formal dispute resolution through their respective chains of command or at their option, escalate the issue to the ISGC. If resolution is not achieved at the ISGC, the Parties may escalate the dispute to the CJCC in an effort to obtain resolution. This Agreement may be enforced in the Circuit Court for the 22nd Judicial Circuit or any other court of the State of Missouri with competent jurisdiction.

ARTICLE V. MODIFICATION OF THE INTERAGENCY AGREEMENT ON INFORMATION SHARING

This Agreement may be amended as follows:

5.1 Any CJCC Member may propose modifications to this Agreement by providing written notice to the ISGC and all CJCC Members detailing the proposed modifications. The ISGC will consider all proposed modifications in good faith, provided that the ISGC may not vote on any proposed modification until at least 30 days following the giving of such notice to all CJCC Members. Upon approval by a majority vote of the ISGC, the proposed modification will be submitted to the CJCC for final approval by a two-thirds majority of the CJCC. Any amendment to this Agreement adopted pursuant to the foregoing process will be binding upon each CJCC Member, whether or not executed by all CJCC Members.

5.2 Alternatively, this Agreement may be amended by written agreement approved by the CJCC and executed and delivered by all CJCC Members.

This Agreement may not otherwise be amended.

ARTICLE VI. GOVERNING LAWS

6.1 This Agreement will be governed by the laws of the State of Missouri. Parties are required to comply with Federal and local regulations and statutes regarding access or dissemination of data, including criminal history and individual privacy, including, without limitation, Title 42 CFR Part 2 and HIPAA. The terms of this Agreement are to be construed in a manner consistent with such laws and regulations and as they may be amended from time to time, and with any other law governing the confidentiality of data shared through the CJCC. In the event of any conflict between the terms of this Agreement and such laws and regulations, the provisions of such laws and regulations will govern the respective rights and duties of the Parties.

6.2 This Agreement is governed the terms and provisions of 28 C.F.R. Part 20 and 28 U.S.C. § 534 relating to the collection, use, dissemination, and control of CHRI, as adopted by the CJCC.

6.3 The terms of this Agreement are to be construed in a manner consistent with such laws and regulations and as they may be amended from time to time, and with any other law governing the confidentiality of shared information. In the event of any conflict between the terms of this Agreement and such laws and regulations, the provisions of such laws and regulations will govern the respective rights and duties of the parties.

6.4 Nothing contained in this Agreement will be construed to obligate any party to any expenditure or obligation of funds in excess or advance of appropriations, in accordance with the Anti Deficiency Act, 31 U.S.C. § 1341.

ARTICLE VII. TERM AND TERMINATION

7.1 Termination of the Agreement. This Agreement will be effective as of the date first written above. The Agreement will continue in effect until terminated by the CJCC or until the dissolution of the CJCC, whichever occurs first.

7.2 Termination of a CJCC Member. This Agreement will terminate, automatically and without notice, with respect to any CJCC Member upon such person's termination as a member of the CJCC. Termination of this Agreement with respect to any CJCC Member under this Section 7.2 will not terminate the Agreement as to the CJCC or any of the other remaining CJCC Members. Articles II, III, IV, VI, VII, and IX will survive with respect to such CJCC Member.

ARTICLE VIII. MISCELLANEOUS PROVISIONS

8.1 Publicity and Media. Each Party may undertake publicity releases and media interviews in connection with its activities under this Agreement, provided that each CJCC Member will provide prior notice of such activity to the CJCC Executive Committee whenever possible.

8.2 Jointly Drafted. This Agreement will be deemed to have been drafted jointly by the Parties and, in the event of a dispute, will not be construed against any Party on the basis of drafting control.

8.3 Authority to Execute. Each of the undersigned individuals represents and warrants that he or she is expressly and duly authorized to execute this Agreement and to legally bind each Party as set forth in this Agreement.

8.4 No Third-Party Beneficiary. This Agreement will not and is not intended to benefit or to grant any right or remedy to any person or entity that is not a party to this Agreement.

8.5 Notices; Representatives of the Parties. Any notice required to be given to a Party by this Agreement will be in writing and will be delivered in person, by courier service or by U.S. Mail, either first class or certified, return receipt requested, postage prepaid, as follows. The Parties hereby designate the individuals named below as their representative responsible for overall administration of this Agreement.

To City: 1200 Market St., St Louis, MO 63103 Attn: Mayor

To the Sheriff: 1114 Market St., St. Louis, MO 63101 Attn: Sheriff

To the Court: 10 N Tucker Blvd, St. Louis, MO 63101 Attn: Court Administrator

To the Circuit Attorney: 1114 Market St., St. Louis, MO 63101 Attn: Circuit Attorney

To the Public Defender: Woodrail Centre, 1000 West Nifong, Building 7 Suite 100, Columbia, MO 65203 Attn: Director

To the MDoC: 2729 Plaza Dr. P.O. Box 236, Jefferson City, MO 65102 Attn: Director

8.6 Severability. If any provision in this Agreement (or any portion thereof) or the applications of any such provision (or any portion thereof) to any person or circumstance will be held invalid, illegal or unenforceable in any respect by a court of competent jurisdiction, such provision(s) (or portions) will be severed from this Agreement and the invalidity, illegality or unenforceability thereof will not affect any other provision of this Agreement, and this Agreement as modified after severing such language will remain in force and effect.

8.7 Entire Agreement/Paragraph Headings. This Agreement sets forth the entire understanding between the Parties and supersedes all previous agreements, arrangements and understandings among the Parties pertaining to the subject matter hereof, whether written or oral, and may not be amended except as provided herein. This Agreement is intended to be binding up and for the benefit of only the Parties and no term or condition hereof is intended to benefit, nor may any term or condition hereof be enforced by any other party not a party to this Agreement. Paragraph headings are for convenience only and will not be deemed a controlling part of this Agreement.

[signature page follows]

IN WITNESS WHEREOF, the Parties hereto have caused this Intergovernmental Agreement to be executed by duly authorized officers in duplicate originals, one of which is retained by each of the Parties, the day and year as set out by each Party.

CITY OF ST. LOUIS

By_____
Mayor Lyda Krewson
Date_____

CITY OF ST. LOUIS SHERIFF

By_____

Name_____

Title_____

Date_____

TWENTY-SECOND JUDICIAL CIRCUIT COURT

By_____

Name_____

Title_____

Date_____

APPROVED AS TO FORM:

By:_____
Julian Bush, City Counselor

COMPTROLLER:

By:_____
Darlene Green, Comptroller

ATTEST:

By:_____
Dione Flowers, Register

CITY OF ST. LOUIS CIRCUIT ATTORNEY

By_____

Name_____

Title_____

Date_____

MISSOURI STATE PUBLIC DEFENDER

By_____

Name_____

Title_____

Date_____

MISSOURI DEPARTMENT OF CORRECTIONS

By_____

Name_____

Title_____

Date_____

EXHIBIT A

Information Exchange Requirements

User Agency Agreement - this agreement is between the CSA, and a local criminal justice agency that uses CJI from the CSA (including federal, state and local information). This agreement outlines the roles and responsibilities of the individual agency such as screening, connectivity, users, validation, dissertation, etc. This document can be modified with approval from the CSA.

Information Exchange Agreement - this agreement is between two criminal justice agencies. It defines the roles and responsibilities between the two agencies. This is typical for agencies who perform work for another criminal justice agency. An example is a large agency providing dispatch for a small agency. This document can be modified with approval from the CSA.

Management Control Agreement - this is an agreement between a criminal justice agency and a non-criminal justice governmental agency. The non-criminal justice agency performs duties that require the agency to have access to criminal justice information. It again defines the roles and responsibilities of both parties. A typical scenario for this would be a county or city IT agency that processes or provides the infrastructure for a criminal justice agency. St Louis City IT and/or REJIS would be in this category. This document can be modified with approval from the CSA.

CJIS Security Addendum - this is an agreement between a criminal justice agency and a private company. Examples are contracted IT or contracted janitorial service providers. It defines roles and responsibilities for each party. This document cannot be modified. The criminal justice agency cannot outsource their responsibility.

HIPAA Consent Requirements – A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances. The authorization must meet the requirements of 45 CFR 164.508.

A covered entity may voluntarily choose, but is not required, to obtain the individual's consent for it to use and disclose information about him or her for treatment, payment, and health care operations. A covered entity that chooses to have a consent process has complete discretion under the Privacy Rule to design a process that works best for its business and consumers. A "consent" document is not a valid permission to use or disclose protected health information for a purpose that requires an "authorization" under the Privacy Rule (see 45 CFR 164.508), or where other requirements or conditions exist under the Rule for the use or disclosure of protected health information.

Business Associate Agreement – A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care

clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules. See the definition of "business associate" at 45 CFR 160.103. Business Associate Agreements are generally required where a covered entity discloses protected health information to the business associate. See 45 CFR 164.504.

Disclosure of Alcohol and Drug Abuse Patient Records - Unlike HIPAA, which generally permits the disclosure of protected health information without patient consent or authorization for the purposes of treatment, payment, or health care operations, 42 CFR Part 2, with limited exceptions (i.e., medical emergencies and audits and evaluations), requires patient consent for such disclosures (42 CFR §§ 2.3, 2.12, 2.13). Some types of exchange, however, may take place without patient consent when a qualified service organization agreement (QSOA) exists or when exchange takes place between a Part 2 program and an entity with administrative control over that program. Note that the subject patient can revoke her/his consent in writing, the initial signed consent needs to have language with that revocation right.

Health Information Exchange - Electronic health information exchange allows doctors, nurses, pharmacists, other health care providers, and patients to appropriately access and securely share an individual's health information—improving the speed, quality, safety, and cost of patient care. Health information exchange can greatly improve the completeness of patient records, which in turn contributes to more informed decision-making at the point of care. Two common types of health information exchange include directed exchange and query-based exchange.

Directed Exchange. Directed exchange enables health care providers to securely send/receive patient information—such as laboratory orders and results, patient referrals, or discharge summaries— via the internet to/from a known and trusted recipient. Common forms of directed exchange include Direct Secure Messaging (commonly compared to secure email for healthcare), point-to-point interfaces between systems, and web services.

Query-Based Exchange. Query-based exchange enables health care providers to search clinical data sources and discover information about a patient. Query-based exchange typically involves an intermediary, often known as a health information exchange (HIE). The HIE either maintains a centralized data repository that includes data from connected systems, or facilitates requests from one system to search another system.

Information Exchange Agreement

Between the

[Criminal Justice Agency]

And the

[Second Criminal Justice Agency]

This Information Exchange Agreement is made and entered into this ___ th day of _____, _____ by and between [Criminal Justice Agency] hereinafter referred to as [CJA Abbreviation] and the [Second Criminal Justice Agency] hereinafter referred to as [CJA 2 Abbreviation].

DEFINITIONS

For the purposes of data control, security and protection and this agreement the [CJA Abbreviation] defines all data provided to or processed by [CJA 2 Abbreviation] on behalf of the [CJA Abbreviation] to be considered Criminal Justice Information (CJI) as defined by, and thus afforded the protections of FBI CJIS Security Policy, Missouri Uniform Law Enforcement System (MULES) Policy and [CJA Abbreviation] polices governing the handling, disclosure and control of the data.

PURPOSE OF AGREEMENT

This agreement defines appropriate security controls and use restrictions for the exchange of criminal justice information between [CJA Abbreviation] and [CJA 2 Abbreviation]. This agreement ensures that any CJI exchanged between [CJA Abbreviation] and [CJA 2 Abbreviation] shall at all times be stored, processed and transmitted in compliance with applicable standards found in FBI CJIS Security Policy, MULES Policy and [CJA Abbreviation] policy.

Duties of [CJA Abbreviation]

Under the terms of this agreement [CJA Abbreviation] shall have the authority to set, maintain and enforce the following duties and standards over and/or relating to the use of and security controls over all CJI and [CJA Abbreviation] provided, obtained or owned data and associated processing systems:

a. The [CJA Abbreviation] shall retain final control over, and retain ownership of, any CJI shared by [CJA Abbreviation] through the exchange received by [CJA 2 Abbreviation].
b. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, applications and other components that comprise and support a telecommunications network and related Criminal Justice and CJIS systems used to process, store, or transmit CJI through the exchange.
c. [CJA 2 Abbreviation] compliance with all applicable federal, state and local laws, FBI CJIS Security Policy, Missouri State Highway Patrol (MSHP) MULES policy and local department policy as they relate to the exchange of CJI between [CJA Abbreviation] and [CJA 2 Abbreviation].
d. Standards for the authorization of [CJA 2 Abbreviation] personnel, contractors, visitors or others who may have access to [CJA Abbreviation] data.

Duties of [CJA 2 Abbreviation]

As a member of this exchange, [CJA 2 Abbreviation] may only access/use the data provided to [CJA 2 Abbreviation] by [CJA Abbreviation] as explicitly authorized in writing as a part of the contract to perform specific

functions on behalf of [CJA Abbreviation], this agreement or another fully executed agreement between these two parties. Additionally, [CJA 2 Abbreviation] may only provide access to [CJA Abbreviation] criminal justice data with the permission of [CJA Abbreviation] as permitted under this agreement, applicable federal and state law, FBI CJIS Security Policy, MULES policy and any other applicable agreements or contracts executed between both parties of this agreement.

CJIS Connectivity

The type of electronic equipment used by [CJA 2 Abbreviation] shall be compatible with the standards set forth in the FBI CJIS Security Policy and shall meet with the approval of the MSHP Information Security Officer (ISO) and the [CJA Abbreviation] Local Agency Security Officer (LASO). [CJA 2 Abbreviation] must receive written approval before granting any access to the [CJA Abbreviation] owned CJI to any agency other than [CJA Abbreviation] or subunits thereof. All such interfaces or connections must also meet all FBI and MSHP CJIS technical specifications and security safeguards.

Screening of [CJA 2 Abbreviation] Personnel and Contractors

All [CJA 2 Abbreviation] employees and contractors with either physical or logical access to CJI and/or unescorted access to terminals processing CJI must submit to a fingerprint-based background check pursuant to MSHP CJIS fingerprint policy. Fingerprints must be submitted to either the [CJA Abbreviation] or the Missouri State Highway Patrol CJIS Division within thirty (30) days of hire. All final determinations for [CJA 2 Abbreviation] employee or contractor access to [CJA Abbreviation] CJI are at the discretion of the MSHP CJIS Systems Officer (CSO) or the TAA of [CJA Abbreviation]. Decisions to approve or deny access will be provided to the [CJA 2 Abbreviation] in writing. A list of authorized [CJA 2 Abbreviation] employees/contractors will be maintained by [CJA 2 Abbreviation] for retrieval during audit.

Dissemination

Any [CJA 2 Abbreviation] employee or contractor who has access to or receives CJI shall only use the access and data for the purposes for which access was required and it will not be disseminated to any other party without explicit permission from the [CJA Abbreviation].

Audit

[CJA 2 Abbreviation] computer equipment, facilities, policies and procedures as well as agency-owned data are subject to and shall be made available for Policy Compliance Reviews, Technical Security Audits and routine review by [CJA Abbreviation] staff, MSHP CJIS auditors or FBI CJIS auditors. [CJA 2 Abbreviation] must allow the aforementioned personnel necessary access to audit, implement and enforce security control as defined by FBI CJIS Security Policy.

Security

[CJA 2 Abbreviation] agrees to limit access to CJI owned by [CJA Abbreviation] or derived from MSHP or FBI CJIS in strict accordance with NCIC, NLETS, MULES, FBI CJIS Security and [CJA Abbreviation] policies and regulations. [CJA 2 Abbreviation] agrees to take full responsibility for the integrity of the CJI stored or processed by [CJA 2 Abbreviation] as a part of this exchange with [CJA Abbreviation]. All [CJA 2 Abbreviation] personnel or contractors with direct or indirect physical or logical access to CJI shall complete security awareness training pursuant to FBI CJIS Security Policy every two (2) years. [CJA 2 Abbreviation] is also responsible for implementing adequate physical security measures at their facilities to protect against any unauthorized personnel gaining access to computer systems, network equipment, storage devices or areas containing/processing CJI. [CJA 2 Abbreviation] shall not provide

any CJI nor allow any contractors or employees thereof to extract any metadata from [CJA Abbreviation] provided CJI except within the official scope of duties performed under this agreement.

Network Diagram

[CJA 2 Abbreviation] is responsible, based on FBI CJIS Security Policy, for providing a network diagram depicting the[CJA 2 Abbreviation] network configuration including the location of all computer equipment, connectivity to [CJA Abbreviation] as well as the data flow/storage within the [CJA 2 Abbreviation] network. This network diagram must be updated whenever substantial changes occur or at least every three (3) years and submitted to the MSHP ISO for review and approval.

Misuse

[CJA Abbreviation] agrees that any misuse of CJIS systems or CJI obtained by or stored on behalf of [CJA Abbreviation] by [CJA 2 Abbreviation] or [CJA 2 Abbreviation] personnel or contractors is a Class A Misdemeanor pursuant to 576.050 RSMo as well as a security incident and as such must be reported to [CJA Abbreviation] and to the MSHP CSO and ISO.

Indemnification

To the extent the law permits, [CJA 2 Abbreviation] agrees to indemnify and hold harmless [CJA Abbreviation], and their officials and employees from and against any and all claims, demands, actions, suits and proceedings by others, against all liability to others, including but not limited to any liability for damages by reason of or arising out of any false arrest or imprisonment, or any loss, cost, expense and damages, resulting from unauthorized use, or out of, or involving any negligence on the part of [CJA 2 Abbreviation] or [CJA 2 Abbreviation] personnel or contractors in the exercise or use of this agreement.

Suspension of Service

[CJA Abbreviation] reserves the right to suspend all use of CJI owned by or provided through this exchange by [CJA Abbreviation] when any terms of this agreement, or documents incorporated herein are violated by [CJA 2 Abbreviation] or [CJA 2 Abbreviation] employees or contractors. Prior to this suspension of connectivity/data use, [CJA 2 Abbreviation] shall be notified in writing by [CJA Abbreviation] of any alleged violations by [CJA Abbreviation] of this agreement. [CJA 2 Abbreviation] shall then have five (5) business days to provide a written response to [CJA Abbreviation] regarding the notice of violation. If the alleged violation has been satisfactorily resolved use of the data and/or CJIS connections will not be suspended and [CJA Abbreviation] shall provide [CJA 2 Abbreviation] with written documentation of the fact. If the remediation or planned remediation of documented violations does not meet the terms of this agreement [CJA Abbreviation] will notify [CJA 2 Abbreviation] of a suspension date in writing. The suspension date will be no less than ten (10) business days from the date [CJA Abbreviation] notifies [CJA 2 Abbreviation] of the forthcoming suspension. After connectivity and use of the CJI has been suspended, [CJA Abbreviation] shall resume furnishing such access and information to [CJA 2 Abbreviation] upon receipt of satisfactory proof that such violations did not occur or that such violations have been fully corrected or eliminated. If satisfactory proof is not received by [CJA Abbreviation] within thirty (30) days following the suspension this agreement will be considered cancelled by [CJA 2 Abbreviation] for non-compliance and will invoke the cancellation section of this agreement.

Cancellation

[CJA Abbreviation] or [CJA 2 Abbreviation] may cancel this agreement with or without cause upon thirty (30) days' notice in writing to the other party. Upon cancellation any and all data/CJI owned by [CJA Abbreviation] shall be furnished to [CJA Abbreviation] by [CJA 2 Abbreviation] in a mutually agreeable format within (30) days of the receipt

of the cancellation notice. Upon notification by [CJA Abbreviation] to [CJA 2 Abbreviation] that the data has been received in an acceptable format [CJA 2 Abbreviation] shall remove and destroy any [CJA Abbreviation] owned data from any systems, databases or backups thereof operated by [CJA 2 Abbreviation].

Incorporation

The following documents and legislation are incorporated into this Management Control Agreement:

1. NCIC 2000 Operating Manual and related Technical and Operational Updates (TOUs)
2. NCIC 2000 Code Manual
3. Interstate Identification Index (III)/National Fingerprint File (NFF) Operational and Technical Manual
4. FBI CJIS Security Policy, Version 5.2
5. FBI CJIS Security Addendum
6. NLETS User and Technical Guide
7. MULES Policies and Procedures Manual
8. MULES Terminal Agency Coordinator (TAC) Guide
9. MULES On-the-Job Training (OJT) Workbook.
10. MSHP CJIS Purpose Code X Manual
11. MSHP CJIS Policy Compliance Review Reference Manual: Fingerprint-Based Identification for Non-Criminal Justice Purposes.
12. All MSHP CJIS Newsletters
13. Minutes of FBI CJIS Advisory Policy Board Meetings
14. Bylaws for the FBI CJIS Advisory Policy Board and FBI CJIS Working Groups
15. Title 28, CFR, Parts 16;20;25;50;901;906
16. Title 5, USC, Chapter 91
17. Title 28, USC, Sections 552;552a;534
18. Title 42, USC, Chapter 72
19. Title 42, USC, Sections 14611-14616
20. Public Law 92-544
21. RSMo Sections 43.010;43.120;43.401;43.500;43.509;43.515;43.532;43.535;43.543;210.482;221.510;301.230;302.225;304.155;304.158;313.220;388.625;455.101;455.050;455.085;559.107;571.101;571.104;576.050;577.001;577.005;577.023;577.51;589.410;590.010;610.120

Acknowledgement

WE THE UNDERSIGNED, AGREE TO COMPLY WITH THE DUTIES, RESPONSIBILITIES AND TERMS NAMED IN THIS MANAGEMENT CONTROL AGREEMENT. WE UNDERSTAND THAT FAILURE TO COMPLY WITH THESE DUTIES AND RESPONSIBILITIES MAY RESULT IN SANCTIONS BY THE [CJA Abbreviation], MISSOURI CJIS SYSTEMS OFFICER AND/OR THE FBI CRIMINAL JUSTICE INFORMATION SERVICES ADVISORY POLICY BOARD, UP TO AND INCLUDING TERMINATION OF ACCESS TO CJIS.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the date set forth below.

[CJA Abbreviation] Administrator:

Name: _____

Signature: _____

Title: _____

[CJA 2 Abbreviation] Administrator:

Name: _____

Signature: _____

Title: _____

Date: _____ Date: _____

MANAGEMENT CONTROL AGREEMENT

Between the

[Criminal Justice Agency]

And the

[Contracted Non-Criminal Justice Entity]

This Management Control Agreement is made and entered into this ___ th day of _____, _____ By and between [Criminal Justice Agency] hereinafter referred to as [CJA Abbreviation] and the [Contracted Non-Criminal Justice Entity] hereinafter referred to as [NCJA Abbreviation] (if applicable).

DEFINITIONS

(Criminal Justice Agencies should use this section to identify their agency as a criminal justice agency citing the authority under which the agency was created and what criminal justice duties their agency performs. Additionally this section should identify the contracted non-criminal justice entity any applicable establishing statutes or ordinances that may apply to the Non-Criminal Justice Agency. An example of this is as follows:)

[NCJA Abbreviation] was established and governed as a _____ pursuant to _____.

For the purposes of Management Control and applicable security addendums, the [CJA Abbreviation] is recognized as a Criminal Justice Agency (CJA) and [NCJA Abbreviation] is recognized as a Non-Criminal Justice Agency (NCJA) as defined in FBI CJIS Security Policy.

For the purposes of data control, security and protection and this agreement the [CJA Abbreviation] defines all data provided to or processed by [NCJA Abbreviation] on behalf of the [CJA Abbreviation] to be considered Criminal Justice Information (CJI) as defined by, and thus afforded the protections of FBI CJIS Security Policy, MULES Policy and [CJA Abbreviation] polices governing the handling, disclosure and control of the data.

PURPOSE OF AGREEMENT

This agreement provides management control for [CJA Abbreviation], which serves as a criminal justice agency authorized under law to receive, process and store CJI. This management control ensures that any contracted work involving the processing, transmission , storage or sharing of CJI performed by [NCJA Abbreviation] on behalf of [CJA Abbreviation] shall remain under the strict management control of [CJA Abbreviation] according to the terms of this agreement and applicable state and federal policies.

Duties of [CJA Abbreviation]

Under the terms of this agreement [CJA Abbreviation] shall have the authority to set, maintain and enforce the following duties and standards over and/or relating to the access to and control over all CJI and [CJA Abbreviation] provided/obtained or owned data and associated processing systems:

e. The [CJA Abbreviation] shall provide management control over, and retain ownership of, any CJI requested by, entered by or received by any employee of [CJA Abbreviation] or employee of [NCJA Abbreviation] who receives criminal justice data on behalf of [CJA Abbreviation].
f. Access to agency owned criminal justice data and CJIS systems by [NCJA Abbreviation]
g. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, applications and other components that comprise and support a telecommunications network and related Criminal Justice and CJIS systems used to process, store, or transmit CJI or any other agency

owned data guaranteeing the priority, confidentiality, integrity and availability of service needed by the criminal justice community.

h. [NCJA Abbreviation] compliance with all applicable federal, state and local laws, FBI CJIS Security Policy, Missouri State Highway Patrol (MSHP) MULES policy and local department policy as they relate to the contracted duties being performed by the [NCJA Abbreviation] on behalf of [CJA Abbreviation].

i. Standards for the selection, supervision and separation of [NCJA Abbreviation] personnel, contractors, visitors or others who may have access to [CJA Abbreviation] data, CJIS Systems or other CJI.

Duties of [NCJA Abbreviation]

As a NCJA contracted organization, [NCJA Abbreviation] may only perform those functions explicitly delegated to [NCJA Abbreviation] by [CJA Abbreviation] in writing as a part of the contract to perform these duties, this agreement or another fully executed agreement between these two parties. Additionally, [NCJA Abbreviation] may only provide access to CJIS Systems and criminal justice data under the management control of the [CJA Abbreviation] as permitted under this agreement, applicable federal and state law, FBI CJIS Security Policy, MULES policy and any other applicable agreements or contracts executed between both parties of this agreement.

CJIS Connectivity

The type of electronic equipment used by [NCJA Abbreviation] shall be compatible with the standards set forth in the FBI CJIS Security Policy and shall meet with the approval of the MSHP Information Security Officer (ISO) and the [CJA Abbreviation] Local Agency Security Officer (LASO). The use of any CJIS interfaces or connections operated on behalf of [CJA Abbreviation] shall be limited to law enforcement/criminal justice purposes and entities with whom [CJA Abbreviation] have a current agency agreement on file with the MSHP Security Unit. [NCJA Abbreviation] must receive written approval before granting any access to the CJIS interface/connection or data operated/maintained on behalf of [CJA Abbreviation] to any agency other than [CJA Abbreviation] or subunits thereof. All such interfaces or connections must also meet all FBI and MSHP CJIS technical specifications and security safeguards.

Screening of [NCJA Abbreviation] Personnel and Contractors

All [NCJA Abbreviation] employees and contractors with either physical or logical access to CJI and/or unescorted access to terminals processing CJI must each sign an FBI CJIS Security Addendum and submit to a fingerprint-based background check pursuant to MSHP CJIS fingerprint policy. Fingerprints must be submitted to either the [CJA Abbreviation] or the MSHP CJIS Division for inclusion in the Missouri Centralized Vendor File within thirty (30) days of hire. All final determinations for [NCJA Abbreviation] employee or contractor access to CJI are at the sole discretion of the MSHP CJIS Systems Officer (CSO). Decisions to approve or deny access will be provided to the [NCJA Abbreviation] in writing. A list of authorized [NCJA Abbreviation] employees/contractors will be maintained by [CJA Abbreviation] or in the Missouri Centralized Vendor File.

Dissemination

Any [NCJA Abbreviation] employee or contractor who has access to or receives CJI shall only use the access and data for the purposes for which access was required and it will not be disseminated to any other party without explicit permission from the [CJA Abbreviation].

Audit

[NCJA Abbreviation] computer equipment, facilities, policies and procedures as well as agency-owned data are subject to and shall be made available for Policy Compliance Reviews, Technical Security Audits and routine review by [CJA Abbreviation] staff, MSHP CJIS auditors or FBI CJIS auditors. [NCJA Abbreviation] must allow the aforementioned personnel necessary access to audit, implement and enforce security control as defined by FBI CJIS Security Policy.

Security

[NCJA Abbreviation] agrees to limit access to CJI owned by [CJA Abbreviation] or furnished by MSHP or FBI CJIS in strict accordance with NCIC, NLETS, MULES, FBI CJIS Security and [CJA Abbreviation] policies and regulations. [NCJA Abbreviation] agrees to take full responsibility for the integrity of the CJI stored or processed by [NCJA Abbreviation] on behalf of [CJA Abbreviation]. [NCJA Abbreviation] shall not be held responsible for the misuse of CJI by non-[NCJA Abbreviation] personnel/contractors. All [NCJA Abbreviation] personnel or contractors with direct or indirect physical or logical access to CJI shall complete security awareness training pursuant to FBI CJIS Security Policy every two (2) years. [NCJA Abbreviation] is also responsible for implementing adequate physical security measures at their facilities to protect against any unauthorized personnel gaining access to computer systems, network equipment, storage devices or areas containing/processing CJI. [NCJA Abbreviation] must provide a complete copy of all [CJA Abbreviation] owned data upon written request in a mutually agreeable format within thirty (30) days of request to [CJA Abbreviation] to allow for the proper inspection and integrity assurance checks of the data. [NCJA Abbreviation] shall not provide any CJI commercially or extract any metadata for use by [NCJA Abbreviation] except within the official scope of duties performed on behalf of [CJA Abbreviation]. Additionally, all CJI data and backups thereof shall remain the property of and under the control of [CJA Abbreviation].

Network Diagram

[NCJA Abbreviation] is responsible, based on FBI CJIS Security Policy, for providing a network diagram depicting the[NCJA Abbreviation] network configuration including the location of all computer equipment, connectivity to CJIS and [CJA Abbreviation] as well as the data flow within the [CJA Abbreviation] network. This network diagram must be updated whenever substantial changes occur or at least every three (3) years and submitted to the MSHP ISO for review and approval.

Misuse

[CJA Abbreviation] agrees that any misuse of CJIS systems or CJI obtained by or stored on behalf of [CJA Abbreviation] by [NCJA Abbreviation] or [NCJA Abbreviation] personnel or contractors is a Class A Misdemeanor pursuant to 576.050 RSMo as well as a security incident and as such must be reported to [CJA Abbreviation] and to the MSHP CSO and ISO.

Indemnification

To the extent the law permits, [NCJA Abbreviation] agrees to indemnify and hold harmless [CJA Abbreviation], and their officials and employees from and against any and all claims, demands, actions, suits and proceedings by others, against all liability to others, including but not limited to any liability for damages by reason of or arising out of any false arrest or imprisonment, or any loss, cost, expense and damages, resulting from unauthorized use, or out of, or involving any negligence on the part of [NCJA Abbreviation] or [NCJA Abbreviation] personnel or contractors in the exercise or use of this agreement.

Suspension of Service

[CJA Abbreviation] reserves the right to suspend all use of CJI owned by, or any CJIS connection operated on behalf of [CJA Abbreviation] when any terms of this agreement, or documents incorporated herein are violated by [NCJA Abbreviation] or [NCJA Abbreviation] employees or contractors. Prior to the suspension of connectivity/data use, [NCJA Abbreviation] shall be notified in writing by [CJA Abbreviation] of any alleged violations by [NCJA Abbreviation] of this agreement. [NCJA Abbreviation] shall then have five (5) business days to provide a written response to [CJA Abbreviation] regarding the notice of violation. If the alleged violation has been satisfactorily resolved use of the data and/or CJIS connections will not be suspended and [CJA Abbreviation] shall provide [NCJA Abbreviation] with written documentation of the fact. If the remediation or planned remediation of documented violations does not meet the terms of this agreement [CJA Abbreviation] will notify [NCJA Abbreviation] of a suspension date in writing. The suspension date will be no less than ten (10) business days from the date [CJA Abbreviation] notifies [NCJA Abbreviation] of the forthcoming suspension. After connectivity and use of the CJI has been suspended, [CJA Abbreviation] shall resume furnishing such access and information to [NCJA Abbreviation] upon receipt of satisfactory proof that such violations did not occur or that such violations have been fully corrected or eliminated. If satisfactory proof is not received by [CJA Abbreviation] within thirty (30) days following the suspension this agreement will be considered cancelled by [NCJA Abbreviation] for non-compliance and will invoke the cancellation section of this agreement.

Cancellation

[CJA Abbreviation] or [NCJA Abbreviation] may cancel this agreement with or without cause upon thirty (30) days notice in writing to the other party. Upon cancellation any and all data/CJI owned by [CJA Abbreviation] shall be furnished to [CJA Abbreviation] by [NCJA Abbreviation] in a mutually agreeable format within (30) days of the receipt of the cancellation notice. Upon notification by [CJA Abbreviation] to [NCJA Abbreviation] that the data has been received in an acceptable format [NCJA Abbreviation] shall remove and destroy any [CJA Abbreviation] owned data from any systems, databases or backups thereof operated by [NCJA Abbreviation].

Incorporation

The following documents and legislation are incorporated into this Management Control Agreement:

22. NCIC 2000 Operating Manual and related Technical and Operational Updates (TOUs)
23. NCIC 2000 Code Manual
24. Interstate Identification Index (III)/National Fingerprint File (NFF) Operational and Technical Manual
25. FBI CJIS Security Policy, Version 5.2
26. FBI CJIS Security Addendum
27. NLETS User and Technical Guide
28. MULES Policies and Procedures Manual
29. MULES Terminal Agency Coordinator (TAC) Guide
30. MULES On-the-Job Training (OJT) Workbook.
31. MSHP CJIS Purpose Code X Manual
32. All MSHP CJIS Newsletters
33. Title 28, CFR, Parts 16;20;25;50;901;906
34. Title 28, USC, Sections 552;552a;534
35. Title 42, USC, Chapter 72
36. Title 42, USC, Sections 14611-14616
37. RSMo Sections 43.010;43.120;43.401;43.500;43.509;43.515;43.532;43.535;43.543;210.482;221.510;301.230;302.225;304.155;304.158;313.220;388.625;455.101;455.050;455.085;559.107;571.101;571.104;576.050;577.001;577.005;577.023;577.51;589.410;590.010;610.120

Acknowledgement

WE THE UNDERSIGNED, AGREE TO COMPLY WITH THE DUTIES, RESPONSIBLITIES AND TERMS NAMED IN THIS MANAGEMENT CONTROL AGREEMENT. WE UNDERSTAND THAT FAILURE TO COMPLY WITH THESE DUTIES AND RESPONSIBILITIES MAY RESULT IN SACTIONS BY THE [CJA Abbreviation], MISSOURI CJIS SYSTEMS OFFICER AND/OR THE FBI CRIMINAL JUSTICE INFORMATION SERVICES ADVISORY POLICY BOARD, UP TO AND INCLUDING TERMINATION OF ACCESS TO CJIS.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the date set forth below.

[CJA Abbreviation] Administrator:

Name: _____

Signature: _____

Title: _____

Date: _____

[NCJA Abbreviation] Administrator:

Name: _____

Signature: _____

Title: _____

Date: _____

Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into this _____ day of _____, 202_, by _____("Covered Entity") and _____ ("Business Associate").

Recitals

Whereas, Business Associate furnishes services to Covered Entity as described in Section 3.1 of this Agreement.

Whereas, Covered Entity is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and, as such, must comply with the Administrative Simplification Provisions of HIPAA, including the Privacy Rule and the Security Rule, and the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

Whereas, HIPAA requires Covered Entity contract with Business Associate to mandate certain protections for the privacy and security of Protected Health Information.

Whereas, Covered Entity and Business Associate intend for this Agreement to satisfy the requirements of HIPAA and the HITECH Act that specify that the Privacy Rule and the Security Rule be incorporated into business associate agreements.

Whereas, Covered Entity and Business Associate mutually agree to comply with the requirements of the implementing regulations at 45 Code of Federal Regulations ("C.F.R.") Parts 160-64 for the Administrative Simplification provisions of Title II, Subtitle F of HIPAA.

Now, therefore, in consideration of the foregoing, and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

ARTICLE I.
DEFINITIONS

1.1 **Catch-all Definition**. Terms used in this Agreement but not otherwise defined in this Agreement shall have the same meaning as those terms in the Privacy Rule, the Security Rule, and the HITECH Act.

1.2 **Definitions.** The terms "Electronic Protected Health Information" and "Protected Health Information" have the meanings set out in 45 C.F.R. § 160.103. The term "Unsecured Protected Health Information" has the meaning set forth at 45 C.F.R. § 164.402. The term "Required by Law" has the meaning set out in 45 C.F.R. § 164.103. The term "Treatment" has the meaning set out in 45 C.F.R. § 164.501. The term "Authorization" has the meaning set out in 45 C.F.R. § 164.508. Designated Record Set will have the meaning set out at 45 C.F.R.

§ 164.501. The term "Subcontractor" has the meaning set out in 45 C.F.R. § 160.103. The term "Breach" will have the meaning set out at 45 C.F.R. § 164.402.

ARTICLE II.
OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

2.1 **Use and Disclosure of Protected Health Information**. Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required by Law. Business Associate further agrees not to use or disclose Protected Health Information in any manner that would constitute a violation of the Privacy Rule or the HITECH Act if so used or disclosed by Covered Entity. Business Associate agrees to use Protected Health Information solely for Covered Entity's benefit and only for the purpose of performing services for Covered Entity as such services are defined in Section 3.1 of this Agreement, and as necessary to comply with Section 3.1 of this Agreement. Business Associate further agrees that Covered Entity shall retain all rights in Protected Health Information not granted herein.

2.2 **Reasonable and Appropriate Safeguards**. Business Associate will implement administrative, physical and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Rule.

2.3 **Mitigation of Harmful Effects**. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of this Agreement.

2.4 **Reporting of Violations**. Business Associate agrees to report to Covered Entity any known access, use, or disclosure of Protected Health Information that is not authorized by this Agreement and/or any Security Incident of which it becomes aware, as well as any Breach of Unsecured Protected Health Information of which it becomes aware, without unreasonable delay, and in no case later than ten (10) calendar days after discovery. Business Associate further agrees to notify Covered Entity of any suspected access, use, or disclosure of data in violation of any applicable federal or state laws or regulations without unreasonable delay, and in no case later than thirty (30) calendar days after discovery. Business Associate agrees to make any such reports to Covered Entity in writing. In the event of a Breach, if a delay is requested by law enforcement, Business Associate may delay notifying Covered Entity for the applicable timeframe. At the request of Covered Entity, Business Associate agrees to identify the date of the Security Incident, the scope of the Security Incident, Business Associate's response to the Security Incident, and the identification of the party responsible for causing the Security Incident, if known. Business Associate also agrees to provide Covered Entity with sufficient information to permit Covered Entity to comply with Breach notification requirements.

Business Associate shall also comply with Missouri law, as applicable.

2.5 **Breach Pattern or Practice by Business Associate**. Business Associate agrees that if Business Associate knows of a pattern of activity or practice of Business Associate that constitutes a material breach of Business Associate's obligations under this Agreement, Business Associate must take reasonable steps to cure the breach or end the violation. Business Associate agrees that if the steps are unsuccessful, Business Associate must terminate this Agreement, or if termination is not feasible, report the problem to the Secretary.

2.6 **Third Party Agreements**. Pursuant to 45 CFR §§ 164.502(e) and 164.308(b), Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information created, received, transmitted, or maintained by Business Associate on behalf of Covered Entity agrees in writing in a business associate agreement to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

2.7 **Availability of Books and Records**. Business Associate agrees to make Protected Health Information and internal practices, books, records, including policies and procedures relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to Covered Entity or to the Secretary, within twenty (20) days or as designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

2.8 **Access**. Business Associate agrees to provide access, at the request of Covered Entity, within twenty (20) days of such request, to Protected Health Information in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual or an Individual's designee, in order to meet the requirements under 45 CFR § 164.524.

2.9 **Amendment**. Business Associate agrees to make any amendments to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and to take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR § 164.526, within thirty (30) days of the request.

2.10 **Documentation of Disclosures**. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528. Business Associate further agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. At a minimum, the information collected and maintained shall include:

2.10.1. The date of the disclosure;

2.10.2. The name of the entity or person who received Protected Health Information and, if known, the address of the entity or person;

2.10.3. A brief description of Protected Health Information disclosed; and

2.10.4. A brief statement of purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

2.11 **Accounting of Disclosures**. Business Associate agrees to provide to Covered Entity or an Individual, within twenty (20) days, information collected in accordance with Section 2.10 of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528 and the HITECH Act, as determined by Covered Entity. Business Associate agrees that such accounting obligations shall survive termination of this Agreement and shall continue as long as Business Associate maintains Protected Health Information.

2.12 **Requests for Accounting**. In the event that a request for accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate agrees to forward the request to Covered Entity in writing within five (5) days.

2.13 **Minimum Necessary**. Business Associate agrees to request, use, and disclose only the minimum amount of Protected Health Information necessary to accomplish the purpose of the request, use, or disclosure.

ARTICLE III.
PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

3.1 General Use and Disclosure. Except as otherwise limited by this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the purposes of _____. Further, Business Associate is only permitted to use and disclose Protected Health Information, whether in paper form or in electronic form, that it creates or receives on the Company's behalf or receives from the Company (or another business associate of the Company) and to request Protected Health Information on the Company's behalf (collectively, "the Company's Protected Health Information") as follows:

(a) **Functions and Activities on the Company's Behalf.** To perform functions, activities, services, and operations on behalf of the Company as specified in the Agreement.

(b) **Business Associate's Operations.** For Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities, provided that, with respect to disclosure of the Company's Protected Health Information, either:

(i) The disclosure is Required by Law; or

(ii) Business Associate obtains reasonable assurance, evidenced by written contract, from any third party person or entity to which

Business Associate will disclose the Company's Protected Health Information that the person or entity will:

(A) Hold the Company's Protected Health Information in confidence and use or further disclose the Company's Protected Health Information only for the purpose for which Business Associate disclosed the Company's Protected Health Information to the person or entity or as Required by Law; and

(B) Promptly notify Business Associate (who will in turn notify the Company in accordance with this Agreement) (Privacy/Security Breach Investigation and Reporting) of this Agreement) of any instance of which the person or entity becomes aware in which the confidentiality of the Company's Protected Health Information was breached.

(c) **Data Aggregation**. In accordance with 45 CFR 164.504(e)(2)(i)(B), Business Associate may use PHI to provide data aggregation services if and only to the extent such data aggregation is necessary for Business Associate to carry out the functions, activities, services, and operations on behalf of the Company as specified in the Agreement.

(d) **Minimum Necessary.** Business Associate will, in its performance of the functions, activities, services, and operations specified above (Permitted Uses and Disclosures) above, make reasonable efforts to use, to disclose, and to request of the Company only the minimum amount of the Company's Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that Business Associate will not be obligated to comply with this minimum necessary limitation with respect to:

(i) Disclosure to or request by a health care provider for Treatment;

(ii) Use for or disclosure to an individual who is the subject of the Company's Protected Health Information, or that individual's personal representative;

(iii) Use or disclosure made pursuant to an Authorization that is signed by an individual who is the subject of the Company's Protected Health Information to be used or disclosed, or by that individual's personal representative;

(iv) Disclosure to the United States Department of Health and Human Services ("DHHS") in accordance herewith (Inspection of Internal Books, Practices and Records) of this Agreement;

(v) Use or disclosure that is Required by Law; or

(vi) Any other use or disclosure that is excepted from the minimum necessary limitation as specified in the Privacy Rule (as hereinafter defined).

(e) **Prohibition on Unauthorized Use or Disclosure.** Business Associate will neither use nor disclose the Company's Protected Health Information, except as permitted or required by this Agreement or in writing by the Company or as Required by Law. This Agreement does not authorize Business Associate to use or disclose the Company's Protected Health Information in a manner that would violate 45 C.F.R. Part 164, Subpart E "Privacy of Individually Identifiable Health Information" ("Privacy Rule") if done by the Company, except as set forth herein (Business Associates Operations) of this Agreement.

(f) Information Safeguards.

(i) Privacy of the Company's Protected Health Information. Business Associate will develop, implement, maintain, and use appropriate administrative, technical, and physical safeguards to protect the privacy of the Company's Protected Health Information. The safeguards must reasonably protect the Company's Protected Health Information from any intentional or unintentional use or disclosure in violation of the Privacy Rule and limit incidental uses or disclosures made pursuant to a use or disclosure otherwise permitted by this Agreement**.**

(ii) Security of the Company's Protected Health Information. Business Associate will use reasonable and appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to the Company's Electronic Health Information, to prevent use or disclosure of that Electronic Protected Health Information other than as provided for by the Agreement.

(g) Subcontractors. Business Associate will require any of its Subcontractors, to which Business Associate is permitted by this Agreement or in writing by the Company to disclose the Company's Protected Health Information, to agree, as evidenced by written contract, that such Subcontractor will comply with the same privacy and security safeguard obligations with respect to the Company's Protected Health Information that are applicable to Business Associate under this Agreement.

ARTICLE IV.
OBLIGATIONS OF COVERED ENTITY

4.1 **Notification of Limitations**. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

4.2 **Notification of Individual Authorization Revocations**. Covered Entity shall notify Business Associate of any changes in, or revocations of, permission by Individual to use or

disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

4.3 **Notification of Restrictions**. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to, in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

4.4 **Permissible Protected Health Information Disclosures**. Covered Entity will not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

ARTICLE V.

INDIVIDUAL RIGHTS

5.1 Access. Business Associate will, within five (5) days following the Company's request, make available to the Company or, at the Company's direction, to an individual (or the individual's personal representative) for inspection and obtaining copies, the Company's Protected Health Information, in a Designated Record Set, about the individual that is in Business Associate's custody or control.

5.2 Amendment. Business Associate will, upon receipt of written notice from the Company, promptly amend, or permit the Company access to amend, any portion of the Company's Protected Health Information.

5.3 Disclosure Accounting. So that the Company may meet its disclosure accounting obligations under the Privacy Rule:

(a) Disclosures Subject to Accounting. Business Associate will record the information specified herein (Disclosure Information) below ("Disclosure Information") for each disclosure of the Company's Protected Health Information, not excepted from disclosure accounting as specified above (Disclosures Not Subject to Accounting) below, that Business Associate makes to the Company or to a third party.

(b) Disclosures Not Subject to Accounting. Business Associate will not be obligated to record Disclosure Information or otherwise account for disclosures of the Company's Protected Health Information that are expressly excluded from such disclosure accounting requirement as set forth at 45 C.F.R. § 164.528(a)(1).

(c) Disclosure Information. With respect to any disclosure by Business Associate of the Company's Protected Health Information that is not excepted from disclosure accounting herein (Disclosures Not Subject to Accounting) above, Business Associate will record the following Disclosure Information as applicable to the type of accountable disclosure made:

(i) Disclosure Information Generally. Except for repetitive disclosures of the Company's Protected Health Information as specified herein (Disclosure Information for Repetitive Disclosures) below, the Disclosure Information that Business Associate must record for each accountable disclosure is (1) the disclosure date, (2) the name and (if known) address of the entity to which Business Associate made the disclosure, (3) a brief description of the Company's Protected Health Information disclosed, and (4) a brief statement of the purpose of the disclosure.

(ii) Disclosure Information for Repetitive Disclosures. For repetitive disclosures of the Company's Protected Health Information that Business Associate makes for a single purpose to the same person or entity (including the Company), the Disclosure Information that Business Associate must record is either (1) the Disclosure Information specified herein (Disclosure Information Generally) above for each accountable disclosure; or (2) the Disclosure Information specified herein (Disclosure Information Generally) above for the first of the repetitive accountable disclosures, the frequency, periodicity, or number of the repetitive accountable disclosures, and the date of the last of the repetitive accountable disclosures.

(d) Availability of Disclosure Information. Business Associate will maintain the Disclosure Information for at least six (6) years following the date of the accountable disclosure to which the Disclosure Information relates. Business Associate will make the Disclosure Information available to the Company within thirty (30) days following the Company's request for such Disclosure Information to comply with an individual's request for disclosure accounting.

(e) Restriction Agreements and Confidential Communications. Business Associate will comply with any reasonable agreement that the Company makes that either (i) restricts use or disclosure of the Company's Protected Health Information, or (ii) requires confidential or alternate methods of communication about the Company's Protected Health Information, provided that the Company notifies Business Associate in writing of the restriction or confidential or alternate communication obligations that Business Associate must follow. The Company will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential or alternate communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of the Company's Protected Health Information will remain subject to the terms of the restriction agreement.

ARTICLE VI.

BREACH INVESTIGATIONS AND REPORTING

6.1 Business Associate will promptly and thoroughly investigate any suspected Breach of the Company's Unsecured Protected Health Information not permitted by this Agreement, or applicable state and/or federal law.

6.2 Business Associate will notify the Company's HIPAA Privacy Office at the address provided below regarding a Breach of the Company's Unsecured Protected Health Information (a "Privacy Event") without unreasonable delay, but in no event later than three (3) calendar days of discovering that a Breach occurred, regardless if such Privacy Event is discovered by Business Associate or by any Subcontractor of Business Associate. Additionally, Business Associate will use its best efforts to assist with the Company's breach investigation by making a timely written report to the Company's HIPAA Privacy Office on any substantiated investigation of a the Privacy Event. Business Associate will include as much of the information described herein (Privacy/Security Breach Investigations) below as is available at the time the report is written, and will supplement the report with additional information once that information is known. For purposes of this paragraph, a Breach shall be treated as discovered as of the first day on which the Breach is known or should reasonably have been known to Business Associate.

6.3 Business Associate's initial written report concerning a Privacy Event will, at a minimum:

(a) a description of what happened, including the date of the Breach and the date of the discovery and who committed the Breach,

(b) the types of unsecured PHI involved in the Breach,

(c) any steps individuals should take to protect themselves from potential harm from the HIPAA Breach, and

(d) what Business Associate is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches.

(e) Provide any other information to the Company as the Company may request to fulfill its reporting obligations to an affected individual as required under 45 C.F.R. § 164.410.

ARTICLE VII.
TERM AND TERMINATION

7.1 **Term**. This Agreement shall be effective as of _____ and shall terminate when all Protected Health Information provided by Covered Entity to Business Associate is destroyed or returned to Covered Entity, or if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Article VII.

7.2 **Termination for Cause**. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

7.2.1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or

7.2.2. Immediately terminate the Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.

If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary. However, in no event will a disclosure by Business Associate that was authorized by Covered Entity be treated as a material breach.

7.3 Effect of Termination. Except as provided in Paragraphs (b) and (c) of this Section 0, upon termination of this Agreement, for any reason, Business Associate shall will, if feasible, return to the Company or destroy all of the Company's Protected Health Information in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of the Company's Protected Health Information. Business Associate will require any Subcontractor, to which Business Associate has disclosed the Company's Protected Health Information as permitted herein (Subcontractors) of this Agreement, to, if feasible, return to Business Associate (so that Business Associate may return it to the Company) or destroy all of the Company's Protected Health Information in whatever form or medium received from Business Associate, including all copies thereof and all data, compilations, and other works derived therefrom that allow identification of any individual who is a subject of the Company's Protected Health Information, and certify on oath to Business Associate that all such information has been returned or destroyed. Business Associate will complete these obligations as promptly as reasonably possible, but not later than thirty (30) days following the effective date of the termination or other conclusion of the Agreement.

7.4 Procedure When Return or Destruction Is Not Feasible. Business Associate will identify any of the Company's Protected Health Information, including any that Business Associate has disclosed to Subcontractors as permitted by Section 2(e) (Subcontractors) of this Agreement, that cannot feasibly be returned to the Company or destroyed and explain to the Company's satisfaction why return or destruction is infeasible. Business Associate will limit its further use or disclosure of such information to those purposes that make return or destruction of such information infeasible. Business Associate will, by its written contract with any Subcontractor to which Business Associate discloses the Company's Protected Health Information as permitted by Section 2(e) (Subcontractors) of this Agreement, require such Subcontractor to limit its further use or disclosure of the Company's Protected Health Information that such Subcontractor cannot feasibly return or destroy to those purposes that make the return or destruction of such information infeasible. Business Associate will complete these obligations as promptly as reasonably possible, but not later than thirty (30) days following the effective date of the termination or other conclusion of the Agreement.

7.5 **Continuing Privacy and Security Obligation.** Business Associate's obligation to protect the privacy and safeguard the security of the Company's Protected Health Information as specified in this Agreement will be continuous and survive termination, assignment of, or other conclusion of the Agreement and this Agreement.

(a) In the event that Business Associate determines that returning or destroying Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon written notification that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protection of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

(b) The preceding provisions of this Section 0 shall not apply to the extent that Protected Health Information is maintained in the possession of Business Associate in accordance with its record retention procedures. Nevertheless, the protections of this Agreement shall remain in effect as to that Protected Health Information as long as Business Associate retains such Protected Health Information.

ARTICLE VIII.
GENERAL PROVISIONS

8.1 **Intent**. The Parties expressly acknowledge that it is, and shall continue to be, their intent to comply fully with all relevant federal, state, and local laws, rules, and regulations.

8.2 **Cross-References**. A reference in this Agreement to a section in HIPAA, the Privacy Rule, the Security Rule, or the HITECH Act means the section as in effect or as amended.

8.3 **Further Actions**. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule, the Security Rule, HIPAA, and the HITECH Act.

8.4 **Survival of Certain Rights and Obligations**. The rights and obligations of Business Associate under this Agreement shall survive the termination of this Agreement.

8.5 **Waiver**. No provision of this Agreement or any breach thereof shall be deemed a waiver unless such waiver is in writing and signed by the Party claimed to have waived such provision or breach. No waiver of a breach shall constitute a waiver of or excuse any different or subsequent breach.

8.6 **Assignment**. Neither Party may assign any of its rights or delegate or subcontract any of its obligations under this Agreement without the prior written consent of the other Party. Notwithstanding the foregoing, Covered Entity shall have the right to assign its rights and obligations hereunder to any entity that is an affiliate or successor of Covered Entity without the prior approval of Business Associate.

8.7 **Notice**. All notices, requests, demands, and other communications required or permitted to be given or made under this Agreement shall be in writing, shall be effective upon receipt, and shall be sent by personal delivery, certified or registered United States mail with return receipt requested, overnight delivery service with proof of delivery, or facsimile with return facsimile acknowledging receipt. Notices shall be sent to the addresses below.

BUSINESS ASSOCIATE:	COVERED ENTITY:
_____ (Name) _____ (Address) _____ (City/State/Zip) Attention: _____ Telephone No.:_____ Facsimile No.: _____	_____ (Name) _____ (Address) _____ (City/State/Zip) Attention: _____ Telephone No.:_____ Facsimile No.: _____

8.8 **Construction**. Any ambiguity in this Agreement shall be resolved to permit Business Associate to comply with the Privacy Rule, the Security Rule, HIPAA, and the HITECH Act.

8.9 **Invalidity or Unenforceability**. If any provision of this Agreement shall be held invalid or unenforceable, such invalidity or unenforceability shall attach only to such provisions and shall not in any way affect or render invalid or unenforceable any other provision of this Agreement.

8.10 **Inspection of Internal Practices, Books, and Records.** Business Associate will make its internal practices, books, and records relating to its use and disclosure of the Company's Protected Health Information available to the Company and to DHHS to determine the Company and Business Associate's compliance with the Privacy Rule.

8.11 **Entire Agreement**. This Agreement constitutes the complete agreement between Business Associate and Covered Entity relating to the matters specified in this Agreement, and supersedes all prior representations or agreements, whether oral or written, with respect to such matters. No oral modification or waiver of any of the provisions of this Agreement shall be binding on either Business Associate or Covered Entity.

8.12 **Governing Law**. This Agreement shall be governed by and interpreted in accordance with the laws of the State of Missouri, excluding its conflicts of laws provisions. Jurisdiction and venue for any dispute relating to this Agreement shall exclusively rest with the state and federal courts in the county in which Covered Entity is located.

8.13 **Rights**. Nothing in this Agreement shall be deemed to:

8.13.1. Create any rights in third parties; or

8.13.2. Waive the attorney-client, work product, or other privilege between Covered Entity and Business Associate arising under applicable law, except to the limited extent necessary to comply with the requirements of Section 2.7 or applicable law.

In Witness Whereof, the parties hereto have executed this Agreement as of its effective date.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
(Name of Covered Entity)	(Name of Business Associate)
By: _____ (Signature)	By _____ (Signature)
Title: _____	Title: _____
Date: _____	Date: _____