Mississippi Medical Cannabis Program
Confidentiality & Application Programming Interface
User Agreement

I. PURPOSE

WHEREAS, Resulting from Initiative 65 to the Mississippi Constitution being overturned by the Mississippi Supreme Court on May 14, 2021, Senate Bill No. 2095, the Mississippi Medical Cannabis Act ("The Act") was signed into law on February 2, 2022. The Act establishes the medical cannabis program ("the program") in the State and charges the Mississippi State Department of Health ("Department" or "MSDH") with the ultimate authority for oversight of the administration of the medical cannabis program. This authority includes, but is not limited to, licensure of cannabis cultivation facilities, cannabis processing facilities, cannabis transportation entities, cannabis disposal entities, cannabis testing facilities, and cannabis research facilities. MSDH also maintains responsibility for patient, caregiver, and practitioner registries for the program. Additionally, the Act charges MSDH with the selection and certification of a seed-to-sale tracking system for the program. In exercising its authority for the program, MSDH collaborates with the Mississippi Department of Revenue ("MDOR"), the agency charged under the Act with authority to license and regulate medical cannabis dispensaries. MDOR also assesses and collects all applicable medical cannabis-related sales and excise taxes.

WHEREAS, The Act requires each licensed medical cannabis establishment ("Licensee") to utilize a statewide seed-to-sale tracking system certified by MSDH to track medical cannabis from seed or immature plant stage until the medical cannabis is purchased by a registered qualifying patient or registered qualifying caregiver or destroyed.

Licensees are permitted to use a certified provider's secondary software system ("Secondary System") in conjunction with METRC. Working with a certified provider, Licensees may establish an interface between the Secondary System and METRC. This Agreement is required in order for the Department and Provider to communicate information electronically between METRC and the Secondary System.

Licensee and patient information are subject to strict confidentiality. The Department will permit Licensees to communicate information electronically to and from METRC through the Secondary System via an API, but this permission is valid only if the Provider of the Secondary System enters into this Agreement to protect the confidentiality of the information/data contained in METRC and the Department's patient registration system. The Provider agrees to maintain data integrity and to comply with the security requirements set forth in this agreement.

II. PARTIES

This Confidentiality and Application Programming Interface ("API") User Agreement ("Agreement") is made as of this ___day of _20____("Effective Date") by and between the third-party provider ("Provider") the Mississippi State Department of Health ("the Department"), and the medical cannabis establishment licensed by the Department and/or

the Mississippi Department of Revenue ("Licensee"), with respect to the availability of one or more secondary software systems (the "Secondary System," as further defined below). The Provider, Licensee, and the Department (collectively referred to as the "Parties") hereby agree to the following terms and conditions.

III. EFFECTIVE DATE AND NOTICE OF NONLIABILITY

A. The Agreement shall not be effective or enforceable until it is approved and signed by all Parties. The effective date of the agreement is the date of the last signature of the Parties. The Department shall not be responsible for the performance of any of its obligations hereunder, or be bound by any provision, prior to the Effective Date.

B. By entering into this Agreement, the Department (and its licensing partner, the Mississippi Department of Revenue ("MDOR")) is under no obligation to appropriate funds for, or to make any payments to, Provider or any Licensee for any reason. Nor shall any provision in this Agreement be construed as imposing liability on the Department and/or MDOR for any expenses Provider or Licensee may make or incur in connection with this Agreement or the performance of this Agreement. Provider expressly waives any claims asserting liability against the Department and/or MDOR in connection with this Agreement or the performance of this Agreement.

IV. TERM

A. The parties intend for the provisions of this Agreement to remain in effect so long as the Provider remains certified by the Department, in consultation with Metrc, to operate the Secondary System. This Agreement shall expire two years after its effective date unless renewed sooner. It is the responsibility of the Provider to initiate all renewals of this Agreement.

B. In the event of termination or expiration of this Agreement, Provider shall take timely, reasonable, and necessary action to protect and preserve Confidential Information (as defined below) in the possession or control of the Provider. All Confidential Information in the possession or control of Provider shall be immediately returned to the Department, and Provider shall certify that no copies of Confidential Information remain in the possession or control of Provider.

C. The provisions of Section 12, Security Requirements and Incident Response shall survive the termination or expiration of this Agreement.

V. CONSIDERATION

The Parties acknowledge that the mutual promises and covenants contained herein, and other good and valuable consideration are sufficient and adequate to support this Agreement, including, but not limited to, the Department's certification of the Provider.

VI. DEFINITIONS

A. "API" means the Application Programming Interface designed, developed, and maintained by METRC.

B. “API Key” means an alphanumeric code generated through METRC to gain programmatic access to METRC and automatic electronic communication of data and information between Provider's System and METRC. There are two kinds of API Keys:

   i. “Vendor API Key” means an API key that is specific to Provider and Provider’s Secondary System, which must be used in every instance of access to Provider's Secondary System at all times, in combination with the User API Key specific to Licensee(s), in order to gain authorized programmatic access to METRC and automatic communication of data and information between Provider's Secondary System and METRC pertaining to such Licensee(s).

   ii. “User API Key” means an API Key that is specific to a particular Licensee, which only such Licensee is able and authorized to generate and obtain or deactivate. The User API Key may be deactivated by generating a new User API Key. The User API Key is linked directly to that Licensee's METRC account and allows access to that Licensee's METRC data and information.

C. “Metrc LLC” means the company engaged by the Department to design, develop, provide, host and maintain the METRC system, and also includes any successor organization responsible for the statewide seed-to-sale system selected by the Department.

D. “Incident” means an accidental or deliberate event that results in or poses a threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources of the Department, MDOR or patients. Incidents include, but are not limited to: (i) successful attempts to gain unauthorized access to the METRC system or Confidential Information regardless of where such information is located; (ii) unwanted disruption or denial of service attacks; (iii) the unauthorized use of METRC in any way; (iv) any unauthorized access by any person to Confidential Information, or (v) changes to the Department's or MDOR’s system hardware, firmware, or software characteristics without the Department's or MDOR’s knowledge, instruction, or consent.

E. “Real Time” means relating to a system in which input data is processed within one second so that is available virtually immediately as feedback.

F. “METRC” or “METRC system” means the medical marijuana seed –to-sale inventory tracking system developed by Metrc LLC to enable the Department to track all legally grown marijuana from seed to sale and includes any successor inventory tracking system that the Department permits or requires Licensees to utilize.

G. “Payment Card Information (PCI) Data” means any data related to card holders' names, credit card numbers, or other credit card or financial information as may be protected by Mississippi and/or federal law.

H. “Confidential Data” shall mean any information from which an individual may be uniquely identified, including, without limitation, an individual’s name, address, email

address, telephone number, social security number, driver's license number, birth date, account numbers, payment card information, and healthcare information. Confidential information is construed broadly to include Department data, Protected Health Information (PHI)[1], and Personally Identifiable Information (PII)[2].

I. "Provider Agreement" means an agreement between a Licensee and Provider entered for the purpose of providing a Secondary System or Services to the Licensee.

J. "Services" means the services to be performed by Provider for Licensee pursuant to the Provider Agreement in connection with the provision, operation, or maintenance of the Secondary System.

K. "Subcontractor" means any third party engaged by Provider to aid in performance of Provider's obligations to Licensee(s).

L. "Secondary System" means the secondary software system provided by Provider for use by a Licensee. Such systems may be used to collect information to be used by the Licensees in operating their businesses, including, but not limited to, secondary inventory tracking and point of sale systems.

M. "Provider" is an entity certified by the Department to provide a Secondary System.

N. "Licensee" is a Department and/or MDOR licensed medical cannabis establishment as defined by SB 2095 of the 2022 Regular Session of the Mississippi Legislature.

VII. CONFIDENTIAL INFORMATION

A. "Confidential Information" means all information, data, records, and documentary materials that are of a sensitive nature regardless of physical form or characteristics and includes, but is not limited to, non-public State records, sensitive State data, protected State data, personally identifying information (PII), payment card industry (PCI) data, and other information or data concerning individuals and Licensees including financial information such as banking information and social security numbers, which has been communicated, furnished, or disclosed by the State to Provider. Confidential Information includes, but is not limited to, any information obtained by Provider through the interface between the METRC system and the Secondary System. Confidential Information may also include any information disclosed to Provider by Licensee, either directly or indirectly, in writing, orally, or through the communication of data through the API, whenever or however disclosed, including, but not limited to:

i names, addresses, or records of patients' personal information;

[1] Which shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. §160.103.

[2] Which is defined by the United States Government Accountability Office (GAO) as, "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as a medical, education, financial, and employment information" (NIST SP 800-122).

ii patient information or data;
iii PII or PHI;
iv PCI Data;
v any other information that should reasonably be recognized as related to the PII Data of patients;
vi inventory tracking data, reports, or records related to the cultivation, manufacture, distribution, or sale of cannabis or cannabis product, if such data, reports, or records are or are intended to be provided to the State through the METRC system or otherwise;
vii business plans and performance related to the past, present, or future activities of such party, its affiliates, subsidiaries, and affiliated companies;
viii all types of Licensee data, including, but not limited to, names and lists of other license holders, service providers, or affiliates;
ix business policies, practices, and procedures;
x names of employees;
xi and any other information that should reasonably be recognized as related to business conducted by a Licensee.

B. Any request or demand, including subpoenas and any public record requests, by a third party for Confidential Information in the possession or control of Provider, shall be immediately forwarded to the Department's Medical Cannabis Program Director or her designee by the recipient of the request. The Department shall follow its business practices for releasing such information.

VIII. AUTHORIZATION

The Department hereby authorizes Metrc LLC to provide a Vendor API Key to Provider that must be used in combination with a Licensee's User API Key to furnish Provider access regarding Licensee's Patient information in the METRC system. This API key is used for the purposes of communicating real-time information to the METRC system. The authorization is granted for use by Licensee(s) in operating the business of such Licensee(s). This Agreement, and Provider's rights and obligations hereunder, shall not be assigned without the prior written consent of the Department, which may be approved or denied in the Department's sole discretion. Authorization by this Agreement grants Licensee the ability to Revoke a Vendor's API Key and requires a reconciliation process and accountability. Provider agrees to accept and abide by the current Metrc Web API Documentation Best Practices, which can be found at https://api-md.metrc.com/documentation#getting-started.

IX. REVOKING A PROVIDER'S API KEY

A Licensee shall have the right to block a Provider's access to its data in METRC by deactivating such Licensee's User API Key and generating a new one or having Metrc LLC generate a new User API Key through METRC.

X. RECONCILIATION & ACCOUNTABILITY

A. A Licensee shall be responsible for ensuring all point-of-sale transactions are accurately represented in the METRC system. Daily verification of reconciliation

should occur to ensure proper reporting. Upon request, the Licensee shall provide the Department with reporting verification that all POS transactions have been reconciled. The Provider of this agreement agrees to ensure their system can provide such reporting verification to Licensee. The Department, either directly or through its agent or designee, may perform an audit of such reconciliations.

B. The Provider further agrees to operate in good faith at all times when providing a System or Service that interfaces with the METRC system.

C. The Department, at its sole discretion, retains the right to revoke or withdraw a vendor API key at any time for any reason set forth by the terms of use in this Agreement.

D. Any entity signing this Agreement is subject to any State of Mississippi, MDOR or Department rules and regulations defining the integrity and accuracy of data entered into METRC. Information entered into the system inaccurately or in violation of the State's, MDOR's or Department's rules or regulations could result in the Department's revocation of a Vendor's API key.

E. Misrepresentation or knowingly entering false information into the Department's tracking system may result in the revocation of the vendor API key and potential violations and penalties associated with the Department's and/or MDOR's rules and regulations associated with the Medical Cannabis Program.

F. API keys are non-transferable and cannot be shared. Sharing an API key with any entity outside of the legal entity, upon discovery, will result in the loss of the API key. Data entered into the API should be done on a transactional / real-time basis. The Vendor is required to perform a "GET" call on available dispensing limits before dispensing product to a patient or caregiver to prevent dispensing of product over that patient's certified limit. "Transactional" data is required to be entered into METRC via the UI, API, or any other means on a "real –time," or as close as possible to real-time, basis.

XI. SECURITY REQUIREMENTS AND INCIDENT RESPONSE

A. The Provider agrees to abide by all applicable federal, State and local laws concerning information security and comply with applicable State of Mississippi, MDOR and Department information security policies. Provider shall limit access to and possession of Confidential Information to only those employees whose responsibilities reasonably require such access or possession and shall train such employees on the Confidentiality obligations set forth herein.

B. The Provider agrees to notify the Department when any Provider system that may access, process, or store Department data or Department systems is subject to unintended access or attack. Unintended access or attack includes compromise by a computer malware, malicious search engine, credential compromise, or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures.

C. The Provider further agrees to notify the Department and MDOR within twenty-four

(24) hours, or earlier, if possible, of the discovery of the unintended access or attack by providing notice via written or electronic correspondence to the Medical Cannabis Program Director or her designee, and the MDOR Alcoholic Beverage Control Chief of Enforcement.

D. The Provider agrees to notify the Department and MDOR within two (2) hours if there is a threat to Provider's product as it pertains to the use, disclosure, and security of the Department's or MDOR's data.

E. If an unauthorized use or disclosure of any Confidential Information occurs, the Provider must provide written notice to the Department and MDOR as soon as possible, but in no event more than one (1) business day, after Provider's discovery of such use or disclosure, and the notice shall identify:

i. the nature of the unauthorized use or disclosure;
ii. the Confidential Information used or disclosed,
iii. who made the unauthorized use or received the unauthorized disclosure;
iv. what the Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and
v. what corrective action the Provider has taken or shall take to prevent future similar unauthorized use or disclosure. The Provider shall provide such other information, including a written report, as reasonably requested by the Department and/or MDOR.

F. The Provider shall protect Confidential Information according to a written security policy no less rigorous than that of the Department and shall supply a copy of such policy to the Department for validation. The Provider agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of Confidential Information or other event requiring notification. In the event of a breach of any of the Provider's security obligations or other event requiring notification under applicable law, the Provider agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless, and defend the Department and MDOR and their officials and employees from and against any claims, damages, or other harm related to such security obligation breach or other event requiring the notification.

G. The Provider shall disclose all of its non-proprietary security processes and technical limitations to the Department.

H. This Section Eleven (11) shall survive expiration or termination of this Contract.

XII. SECURITY INCIDENT OR DATA BREACH NOTIFICATION

A. In accordance with Section 11 above, the Provider shall immediately inform the Department and MDOR of any security incident or data breach.

B. Incident Response: The parties acknowledge that the Department, MDOR and the Provider may need to communicate with outside parties regarding any security incident, which may include contacting law enforcement, addressing media inquiries,

and seeking external expertise. Provider shall treat all communications with the Department and MDOR regarding such matters as urgent. The Provider shall discuss and coordinate any such response and communications with the Department and MDOR.

C. Breach Reporting Requirements: If the Provider has actual knowledge of a confirmed data breach that affects the security of any Department or MDOR content, if applicable in the situation, the Provider shall (1) promptly notify the appropriate Department and MDOR-identified contact within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner and in accordance with applicable laws.

D. Unless otherwise stipulated, if a data breach is a direct result of the Provider's breach of its obligation to properly encrypt Confidential Data or otherwise prevent its release, the Provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators, or others required by the Department, MDOR or by law; (3) a credit monitoring service as determined by the Department; (4) a website or a toll- free number and call center for affected individuals as directed by the Department; and (5) completing all corrective actions as reasonably determined by Provider to address the root cause of the data breach.

XIII. DATA PROTECTION

A. Data Ownership- The Department or MDOR will own all rights, title, and interest in its data that is related to this Agreement, as applicable. The Provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations (2) in response to service or technical issues, (3) as required by the express terms of this agreement, or (4) at the Department's written request.

B. Loss of Data- In the event of loss of any Department or MDOR data or records where such loss is due to the intentional act, omission, or negligence of the Provider or any of its subcontractors or agents, the Provider shall be responsible for recreating such lost data in the manner and on the schedule set by the Department or MDOR, as applicable. The Provider shall ensure that all data is backed up and is recoverable by the Licensee. In accordance with prevailing federal or Mississippi law or regulations, the Provider shall report the loss of non-public data as directed in this agreement.

C. Protection of data and personal privacy (as further described and defined in this agreement) shall be an integral part of the business activities of the Provider to ensure there is no inappropriate or unauthorized use of Department or MDOR information at any time. To this end, the Provider shall safeguard the confidentiality, integrity, and availability of Department and MDOR information as further indicated in this section.

D. The Provider shall implement and maintain appropriate administrative, technical, and organizational security measures to safeguard against unauthorized access, disclosure, or theft of Confidential Information and non-public data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Provider applies to its own Confidential Information and non-public data

of similar kind.

E. All Confidential Information shall be encrypted at rest and in transit with controlled access, including back-ups. Unless otherwise stipulated, the Provider is responsible for the encryption of the Confidential Information. All data collected or created in the performance of this contract shall become and remain property of the Department.

F. Unless otherwise stipulated, the Provider shall encrypt all non-public data at rest and in transit. The Department shall identify to the Provider the data it deems non-public. The level of protection and encryption for all non-public data shall be identified and made a part of this Agreement.

G. At no time shall any data or processes – that either belong to or are intended for the use of the Department or its officers, agents or employees – be copied, disclosed, or retained by the Provider or any party related to the Provider for subsequent use in any transaction that does not include the Department.

H. The Provider shall not use any information, whether it be in the aggregate or related to specific individuals, collected in connection with the service issued under this Agreement for any purpose other than fulfilling the service. Data and any information collection in connection with this service shall not be used, sold, or transferred for promotional or any other purposes.

I. The Provider and Licensee must take all reasonable precautions to protect against unauthorized access or release of customer data records, confidential records, or confidential information in the custody of the Provider and/or Licensee. Provider and Licensee shall comply with the Notice Sections of the Department's Business Associate Agreement attached to this agreement as Exhibit A.

XIV. ADDITIONAL TERMS REGARDING DATA

A. Data Location -The Provider shall provide its services to the Department and its end users solely from data centers in the United States ("U.S."). Storage of Department data at rest shall be located solely in data centers in the U.S. The Provider shall not allow its personnel or contractors to store Department data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Provider shall permit its personnel and contractors to access Department data remotely only as required to provide technical support. If requested by the Department, the Provider shall provide technical user support on a 24/7 basis.

B. Import and Export of Data- The Department shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Provider. This includes the ability for the Department to import or export data to/from third parties.

C. Encryption of Data at Rest- The Provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Confidential Data, unless the Department approves the storage of Confidential Data on a Provider portable device in

order to accomplish System services.

D. Release of Data- The Provider shall contact the Department and/or MDOR upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to the Department's and/or MDOR's data under this Agreement, or which in any way might reasonably require access to the data of the Department and/or MDOR, unless prohibited by law from providing such notice. The Provider shall not respond to subpoenas, service of process and other legal requests related to the Department and/or MDOR without first notifying the Department and/or MDOR, unless prohibited by law from providing such notice.

E. Disposition of Data- The Department and MDOR retain the right to use the System to access and retrieve Confidential Information stored on Provider's infrastructure at the State's sole discretion. Provider warrants, and shall cause each Subcontractor to warrant, that upon request of the State, the Department, MDOR or Provider, such Subcontractor shall submit its data processing facilities for an audit of its compliance with section 13 of this Agreement, including, but not limited to, the measures referred to in section 13. The State reserves its rights, title, and interest, including all intellectual property and proprietary rights, in and to METRC, METRC system data, Confidential Information, and all related data and content.

F. Safeguarding PII Data- If Provider will or may receive PII Data under this Agreement, Provider shall provide for the security of such PII Data, in a form acceptable to the State, including, but not limited to, nondisclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, and audits. Provider shall take full responsibility for the security of all PII Data in its possession and shall hold the State harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof.

G. Safeguarding PCI Data- If Provider will or may receive PCI Data under this Agreement, Provider shall provide for the security of the PCI Data, in accordance with PCI Data Security Standard (DSS) 1.1. Security safeguards shall include, without limitation, supervision by responsible employees, approval of Subcontractors as required by State and/or federal law, non-disclosure of information other than as necessary in the performance of Provider's or Subcontractor's obligations under this Agreement, non- disclosure protections, proper accounting and storage of information, civil and criminal penalties for non-compliance as provided by law, certifications, and inspections.

XV. REMEDIES

A. If Provider is in breach under any provision of this Agreement, the Department and/or MDOR shall have all remedies available under the law including, but not limited to, those remedies expressly set forth in this Agreement. The Department and/or MDOR may exercise any or all of the remedies available to it under the law, in its sole discretion, concurrently or consecutively.

B. Vendor API Key Deactivation- Upon any breach of this Agreement, the Department

may deactivate Provider's Vendor API Key. Provider agrees that the Vendor API Key does not constitute any ownership and expressly waives any rights associated with the provision of information obtained with API Key.

C. Damages- Notwithstanding any other remedial action by the Department, Provider shall remain liable to the Department and/or MDOR for any damages sustained by the Department and/or MDOR by virtue of any breach under this Agreement by Provider.

D. Early Termination in the Public Interest- If this Agreement ceases to further the public policy of the Department, the Department, in its sole discretion, may deactivate Provider's Vendor API Key and terminate this Agreement. Exercise by the Department of this right shall not constitute a breach of the Department's obligations hereunder.

E. Remedies Not Involving Termination - The Department, in its sole discretion, may exercise the following remedies in addition to other remedies available to it:

   i. Removal- Notwithstanding any other provision herein, the Department may demand immediate removal of any of Provider's employees, agents, Subcontractors, or permitted assigns whom the Department deems incompetent, careless, insubordinate, unsuitable, or otherwise unacceptable, or whose continued relation to this Agreement is deemed to be contrary to the public interest or the Department's best interest.

   ii. Intellectual Property- If Provider infringes on a patent, copyright, trademark, trade secret, or other intellectual property right while performing the Services or providing the System, Provider shall, at the Department's option (a) obtain the right to use such products and Services; (b) replace any goods, Services, or product involved with non-infringing goods, Services or products or modify such goods, Services or products so that they become non-infringing; or (c) if neither of the foregoing alternatives are reasonably available, remove any infringing goods, Services, or products.

F. Licensee shall have the right to block a Provider’s access to its data in METRC be deactivating such licensee’s User API key.

G. In addition to remedies listed in this section, the following schedule shall be used when administratively disciplining medical cannabis establishments for statutory or regulatory violations. The Department and/or MDOR, as applicable, reserve the right to increase penalties based on aggravating circumstances, and any conflict between the penalties as listed in this agreement and regulatory schedules of disciplinary action shall be governed by the regulatory schedule. Penalties may also be applied to Providers in accordance with the terms of this agreement.

Violation	First Offense	Second Offense	Third Offense
Negligent failure to accurately track inventory	$5,000.00	$10,000.00 and one week suspension	$20,000.00 and two month suspension
Willful failure to accurately track inventory	$10,000.00 and one week suspension	$20,000.00 and two month suspension	Revocation

XVI. INDEMNIFICATION

A. Provider shall indemnify, defend, and hold the Department and MDOR their board members, directors, officers, employees, representatives, and agents, and the State of Mississippi, harmless against all claims, demands, suits, action, damages, losses, costs and liabilities of every kind and nature whatsoever, arising out of or caused by Provider and/or its partners, principals, agents, employees and /or subcontractors in the performance of or failure to perform this agreement including, but not limited to (a) tangible property damage, bodily injury and death, to the extent caused or contributed to by the Provider, (b) for the fraud or willful misconduct of the Provider, and (c) for the negligent, whether intentional or unintentional, misconduct of the Provider, and such indemnifications shall include all related defense costs and expenses (including reasonable attorneys' fees and costs of investigation, litigation, settlement, judgments, interest and penalties) arising from or relating to the performance of the Provider or its Subcontractors under this Agreement.

B. Neither the Department nor MDOR has any obligation to provide legal counsel or defense to the Provider or its Subcontractors in the event that a suit, claim, or action of any character is brought by any person not party to this Agreement against the Provider or its subcontractors as a result of or relating to the Provider's obligations under this Agreement.

C. Neither the Department nor MDOR has any obligation for the payment of any judgments or the settlement of any claims against the Provider or its Subcontractors as a result of or relating to the Provider's obligations under this Agreement. The Provider shall immediately notify the Department and MDOR of any claim or suit made or filed against the Provider or its Subcontractors regarding any matter resulting from or relating to the Provider's obligations under the Agreement and will cooperate, assist, and consult with the Department and/or MDOR, as applicable, in the defense or investigation of any claim, suit, or action made or filed by a third party against the Department or MDOR as a result of or relating to the Provider's performance under this Agreement.

XVII. TERMINATION

The Department may terminate this entire Agreement or any part of this Agreement.

Exercise by the Department of this right shall not be a breach of its obligations hereunder. Provider shall continue performance of this Agreement to the extent not terminated, if any.

To the extent specified in any termination notice, Provider shall take timely, reasonable, and necessary action to protect and preserve Confidential Information in the possession or control of the Provider. All Confidential Information in the possession or control of Provider shall be immediately returned to the State as specified in this Agreement and Provider shall certify that no copies of Confidential Information remain in the possession or control of Provider.

XVIII. EMPLOYEE FINANCIAL INTEREST/ CONFLICT OF INTEREST

The signatories of this agreement have no knowledge of a State employee having any personal or beneficial interest whatsoever in the System or Services described in this Agreement. Provider has no interests and shall not acquire any interest, direct or indirect, that would conflict in any manner or degree with the performance of Provider's Services and Provider shall not employ any person having such known interests.

See next page for applicable law and signatures

XIX. APPLICABLE LAW

This agreement shall be governed and construed in accordance with the laws of the State of Mississippi, excluding its conflicts of law provisions, and any litigation with respect here to shall be brought in the appropriate court of Hinds County in the State of Mississippi. Parties shall comply with applicable federal, state, and local laws and regulations.

Each party set forth below agrees to be bound by the terms of this Agreement as of the effective date.

Mississippi State Department of Health

_____
Signature

_____
Printed Name

_____
Title

_____
Date

Licensee

_____
Signature

_____
Printed Name

_____
Title

_____
Date

Provider

_____
Provider Entity Name

_____
Signature

_____
Printed Name

_____
Title

_____
Date

Exhibit A

MISSISSIPPI STATE DEPARTMENT OF HEALTH BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement is entered into by and between the Mississippi State Department of Health ("MSDH") the Covered Entity and _____ ("Business Associate"), hereinafter referred to as the Parties, and modifies any other prior existing agreement or contract for this purpose. In consideration of the mutual promises below and the exchange of information pursuant to this Agreement and in order to comply with all legal requirements for the protection of this information, the Parties therefore agree as follows:

I. RECITALS

a. MSDH is a state agency with a principal place of business at 570 East Woodrow Wilson, Jackson, MS 39215

b. Business Associate is a corporation qualified to do business in Mississippi that will act to perform business services for MSDH with a principal place of business at _____ _____.

c. This Business Associate Agreement ("Agreement") is entered into pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, as amended by the Genetic Information Nondiscrimination Act ("GINA") of 2008 and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), Title XIII of Division A, and Title IV of Division B of the American Recovery and Reinvestment Act ("ARRA") of 2009, and its implementing regulations, including, but not necessarily limited to, 45 C.F.R. Part 160, and 45 C.F.R. Part 164 Subparts A and C ("Security Rule"), and 45 C.F.R. Part 160 Subparts A and E ("Privacy Rule"). These statutes and regulations are hereinafter collectively referred to as HIPAA. MSDH, as a covered entity, is required to enter into this Agreement to obtain satisfactory assurances that Business Associate will comply with and appropriately safeguard all Protected Health Information ("PHI") Used, Disclosed, created, or received by Business Associate on behalf of MSDH. Certain provisions of HIPAA and its implementing regulations apply to Business Associate in the same manner as they apply to MSDH, and such provisions must be incorporated into this Agreement.

d. MSDH desires to engage Business Associate to perform certain functions for, or on behalf of, MSDH involving the Disclosure of PHI by MSDH to Business Associate, or the creation or Use of PHI by Business Associate on behalf of MSDH, and Business Associate desires to perform such functions, as set forth in the Underlying Agreement(s) which involve the exchange of information, and wholly incorporated herein.

II. DEFINITIONS

a. "Breach" shall mean the acquisition, access, Use or Disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI, and subject to the exceptions set forth in 45 C.F.R. § 164.402.

b. "Business Associate" shall mean _____, including all workforce members, representatives, agents, successors, heirs, and permitted

assigns.

c. "Covered Entity" shall mean the Mississippi State Department of Health, an agency of the State of Mississippi.

d. "Data Aggregation" shall have the same meaning as the term "Data aggregation" in 45 C.F.R. §164.501.

e. "Designated Record Set" shall have the same meaning as the term "Designated Record Set" in 45 C.F.R. §164.501.

f. "Disclosure" shall have the same meaning as the term "Disclosure" in 45 C.F.R. § 160.103.

g. "MSDH" shall mean the Mississippi State Department of Health, an agency of the State of Mississippi.

h. "Individual" shall have the same meaning as the term "Individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

i. "Privacy Officer" shall mean the person designated by MSDH to oversee its implementation of and compliance with HIPAA.

j. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E.

k. "Protected Health Information" or "PHI" shall have the same meaning as the term "Protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of MSDH.

l. "Required by Law" shall have the same meaning as the term "Required by law" in 45 C.F.R. § 164.103.

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

n. "Security Incident" shall have the same meaning as the term "Security incident" in 45 C.F.R. §164.304.

o. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and C.

p. "Standard" shall have the same meaning as the term "Standard" in 45 C.F.R. § 160.103.

q. "Underlying Agreement" shall mean any applicable Memorandum of Understanding ("MOU"), agreement, contract, or any other similar device, and any proposal or Request for Proposal ("RFP") related thereto and agreed upon between the Parties, entered into between MSDH and Business Associate. Under this Business Associate Agreement, "Underlying Agreement" shall refer to the following:

_____.

r. "Unsecured Protected Health Information" shall have the same meaning as the term "Unsecured protected health information" in 45 C.F.R. § 164.402.

s. "Use" shall have the same meaning as the term "Use" in 45 C.F.R. § 160.103

t. "Violation" or "Violate" shall have the same meaning as the terms "Violation" or "Violate" in 45 C.F.R. § 160.103.

All other terms not defined herein shall have the meanings assigned in HIPAA and its implementing regulations.

III. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a. Business Associate agrees to not Use or Disclose PHI other than as permitted or required by this Agreement and the Underlying Agreement(s), or as Required by Law.

b. Business Associate agrees to utilize appropriate safeguards and comply, where applicable, with the HIPAA Privacy and Security Rules, to prevent Use or Disclosure of the PHI other than as permitted or provided for by this Agreement and shall: (i) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Protected Health Information and Electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on behalf of MSDH; (ii) ensure that any subcontractor to whom Business Associate provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (iii) report to MSDH any Security Incident of which Business Associate becomes aware.

c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in Violation of the requirements of this Agreement and/or state or federal laws and regulations.

d. **Breaches and Security Incidents.** During the term of this Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any actual or suspected Breach or Security Incident. Business Associate agrees to take the following steps:

Notice to MSDH. (1) To notify their MSDH Point-of-Contact, MSDH IT Security Officer and MSDH Privacy Officer **without unreasonable delay, and no later than five (5) days after discovery, by telephone call and email or registered or certified mail** upon the discovery of an actual or suspected Breach of Unsecured PHI in electronic media or in any other media. (2) To notify their MSDH Point-of-Contact, MSDH IT Security Officer and MSDH Privacy Officer **without unreasonable delay, and no later than five (5) days after discovery, by telephone call and email or registered or certified mail** of any actual or suspected Security Incident affecting this Agreement, including but not limited to an actual or suspected Security Incident that involves data provided to MSDH by the Social Security Administration. A Breach or Security Incident shall be treated as discovered by Business Associate as of the first day on which the Breach or Security Incident is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the Breach or Security Incident) who is a workforce member, officer, or other agent of Business Associate.

The notification shall include, to the extent possible and subsequently as the information becomes available, a reasonably detailed description of the actual or suspected Breach or Security Incident, the identification of all Individuals whose Unsecured PHI is reasonably believed by Business Associate to have been affected by the Breach or Security Incident along with any other available information that is required to be included in the notification to the Individual, HHS and/or the media, all in accordance with the data breach notification requirements set forth in 42 U.S.C. § 17932 and 45 C.F.R. Parts 160 and 164, Subparts A, D, and E, or any other applicable notification requirements.

Upon discovery of an actual or suspected Breach or Security Incident, Business Associate shall take:

- Prompt corrective action to mitigate any risks or damages involved with the Breach or Security Incident and to protect the operating environment; and

- Any action pertaining to such unauthorized Disclosure required by applicable Federal and State laws and regulations.

Investigation. To immediately investigate any such actual or suspected Breach or Security Incident upon discovery in order to determine if the actual or suspected Breach or Security Incident is a Violation of any applicable federal or state laws or regulations, and to submit updated information by email or registered or certified mail, as it becomes available, to the MSDH IT Security Officer and MSDH Privacy Officer.

Complete Report. To provide a complete written report by email or registered or certified mail of the investigation to the MSDH IT Security Officer and MSDH Privacy Officer within ten (10) working days of the discovery of any actual or suspected Breach or Security Incident. The report shall include:

- the identification of each Individual whose PHI was or is believed to have been involved;

- a reasonably detailed description of the types of PHI involved; and

- a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain any suspected or actual Breach of security, intrusion or unauthorized Use or Disclosure.

If MSDH requests information in addition to that provided in the written report, Business Associate shall make reasonable efforts to provide MSDH with such information. If necessary, a supplemental report may be utilized to submit revised or additional information after the completed report is submitted.

Notification of Individuals. If the cause of an actual Breach of PHI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify each Individual of the Breach when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the Breach. The notifications shall comply with the requirements set forth in 42 U.S.C. § 17932 and its implementing regulations. The MSDH IT Security Officer and MSDH Privacy Officer shall approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made.

Responsibility for Reporting of Breaches. If the cause of a Breach of PHI is attributable to Business Associate or its agents, subcontractors, or vendors, and Business Associate is a covered entity as defined under HIPAA and the HIPAA regulations, Business Associate is responsible for all required reporting of the Breach as specified in 42 U.S.C. § 17932 and its implementing regulations, including notification to media outlets and to the Secretary of the U.S. Department of Health and Human Services. If Business Associate has reason to believe that duplicate reporting of the same Breach or Security Incident may occur because its subcontractors, agents or vendors may report the Breach or Security Incident to MSDH in addition to Business Associate, Business Associate shall notify MSDH, and MSDH and Business Associate may take appropriate action to prevent duplicate reporting. The Breach reporting requirements of this paragraph are in addition to the reporting requirements set forth above.

e. Business Associate agrees to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate with respect to such information, all in accordance with 45 C.F.R. §§ 164.308 and 164.502

f. Business Associate agrees to ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of Business Associate agree to comply with the applicable requirements of the Security Rule and Privacy Rule by entering into a Business Associate Agreement, in accordance with 45 C.F.R. §§ 164.308, 164.314, 164.502, and 164.504, and Business Associate shall provide MSDH with a copy of all such executed agreements between Business Associate and Business Associate's subcontractors. Business Associate understands that submission of their subcontractors' Business Associate Agreement(s) to MSDH does not constitute MSDH approval of any kind, including of the utilization of such subcontractors or of the adequacy of such agreements.

g. Business Associate agrees that nothing in this Agreement is meant to take the place of any HIPAA-mandated reporting duties that apply directly to the Business Associate as a covered entity under HIPAA and its implementing regulations.

h. Business Associate agrees to provide access, at the request of MSDH, and in the time and manner designated by MSDH, to PHI in a Designated Record Set, to MSDH or, as directed by MSDH, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524.

i. Business Associate agrees to document such Disclosures of PHI and information related to such Disclosures as would be required for MSDH to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528. Business Associate agrees to retain such documentation for at least six (6) years after the date of Disclosure; the provisions of this Section shall survive termination of this Agreement for any reason.

j. Where applicable, Business Associate agrees to retain and securely store all data and documents falling under this Agreement and the Underlying Agreement(s) in accordance with HIPAA, the HITECH Act, and their implementing regulations.

k. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that MSDH directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of MSDH or an Individual, and in the time and manner designated by MSDH.

l. Business Associate agrees to provide to MSDH or an Individual, in a time and manner designated by MSDH, information collected in accordance with Section (III) of this Agreement, to permit MSDH to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 C.F.R. § 164.528.

m. Business Associate agrees that it shall only Use or Disclose the minimum PHI necessary to perform functions, activities, or services for, or on behalf of, MSDH as specified in the Underlying Agreement(s). Business Associate agrees to comply with any guidance issued by the Secretary on what constitutes "minimum necessary" for purposes of the Privacy Rule, and any minimum necessary policies and procedures communicated to Business Associate by MSDH.

n. Routine transmission of PHI by fax is not recommended. If information must be faxed, Business Associate agrees PHI shall be limited to those recipients who have a need to gain access to the information. The information to be faxed shall be limited to the "minimum necessary" to accomplish the proposed function. A cover sheet must be utilized which includes a required confidential statement prohibiting unlawful redisclosure. In the event a fax is received by an unintended recipient, Business Associate should obtain the recipient's contact information, attempt to identify the misdirected document, and then contact MSDH Privacy Officer. Generally, Business Associate should instruct the recipient of the misdirected fax to await further instructions from the Business Associate. Recipients should *not* be told to throw away a misdirected fax. MSDH may instruct the recipient to return or destroy the document, depending on the facts.

o. Business Associate agrees that to the extent that Business Associate carries out MSDH's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to MSDH in the performance of such obligation.

p. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the Use and Disclosure of PHI received from, or created or received by Business Associate on behalf of, MSDH available to the Secretary for purposes of determining MSDH's compliance with the Privacy Rule.

q. Business Associate agrees that nothing in this Agreement shall permit Business Associate to access, store, share, maintain, transmit or Use or Disclose PHI in any form via any medium with any third party, including Business Associate's subcontractors, beyond the boundaries and jurisdiction of the United States without express written authorization from MSDH.

r. Business Associate agrees that all MSDH data will be encrypted using industry standard algorithms, preferably AES256 or Triple DES and/or SSL/TLS 1.2+.

s. Business Associate agrees to comply with the State of Mississippi ITS Enterprise Security Policy, which will be provided by MSDH upon request.

t. Business Associate agrees to make an executive summary of its most recent information security audit available to MSDH upon request by MSDH.

u. The provisions of the HITECH Act that apply to Business Associate and are required to be incorporated by reference in a business associate agreement are hereby incorporated into this Agreement, including, without limitation, 42 U.S.C. §§ 17935(b), (c), (d) and(e), and 17936(a) and (b), and their implementing regulations.

v. 42 U.S.C. §§ 17931(b) and 17934(c), and their implementing regulations, each apply to Business Associate with respect to its status as a business associate to the extent set forth in each such section.

w. Business Associate shall be responsible for, and shall reimburse MSDH for costs and expenses associated with steps reasonably implemented by MSDH to mitigate any Breach or other non-permitted Use or Disclosure of PHI or medical, health or personal information protected by other federal or state law, including, without limitation, the following: data analysis to determine appropriate mitigation steps in the event of a Breach, including assistance from Business Associate in the investigation of the Breach and, as needed, access to Business Associate's systems and records for purposes of Breach data analysis; preparation and mailing of notification(s) about the Breach to impacted Individuals, the media and regulators; costs associated with proper handling of inquiries from Individuals and other entities about the Breach (such as the establishment of toll-free numbers, maintenance of call centers for intake, preparation of scripts, questions/answers, and other communicative information about the Breach); credit monitoring and account monitoring services for impacted Individuals for a reasonable period (which shall be no less than 12 months); other mitigation action steps required of MSDH by federal or state regulators; and other reasonable mitigation steps required by MSDH.

x. Business Associate shall not, without written authorization from MSDH, perform marketing or fundraising on behalf of MSDH, or engage in the types of communications on behalf of MSDH that are excepted from the definition of "marketing" established at 45 C.F.R. §164.501. If MSDH requests and authorizes Business Associate to engage in these activities, Business Associate shall comply with the applicable provisions of the HITECH Act and the HIPAA Rules.

y. Business Associate shall not directly or indirectly receive remuneration in exchange for an Individual's PHI unless it is pursuant to specific written authorization by the Individual or subject to an exception established in the HIPAA Rules.

z. Without prior written approval from MSDH, Business Associate shall not publicly release any report, article, paper, graph, chart, or other product created, in whole or in part, using data provided or developed under this Agreement.

aa. Business Associate agrees to utilize reasonable measures (including training) to ensure compliance with the requirements of this Agreement by employees who assist in the performance of functions or activities under this Agreement and Use or Disclose MSDH data,and to discipline such employees who intentionally violate any provisions of this Agreement.

IV. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

a. General Use and Disclosure Provisions: Subject to the terms of this Agreement, Business Associate may Use or Disclose PHI to perform functions, activities, or services for, or on behalf of, MSDH as specified in the Underlying Agreement(s), provided that such Use or Disclosure would not Violate what is Required by Law or the Privacy Rule if done by MSDH, except for the specific Uses and Disclosures set forth below, for the purpose of performing the Underlying Agreement(s).

b. Specific Use and Disclosure Provisions:

i. Business Associate may Use PHI, if necessary, for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate under the Underlying Agreement(s) entered into between MSDH and Business Associate.

ii. Business Associate may 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 and the person to whom the PHI was Disclosed notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

iii. If Business Associate must Disclose PHI pursuant to law or legal process, Business Associate shall notify MSDH by phone and in writing without unreasonable delay and at least five (5) days in advance of any Disclosure so that MSDH may take appropriate steps to address the Disclosure, if needed.

iv. In the event that Business Associate works for more than one covered entity, Business Associate may Use and Disclose PHI for Data Aggregation purposes, however, only in order to analyze data for permitted health care operations, and only to the extent that such is permitted under the Privacy Rule.

v. Business Associate may Use and Disclose de-identified health information if (a) the Use is communicated to MSDH and (b) the de-identified health information meets the implementation specifications for de-identification under the Privacy Rule.

V. OBLIGATIONS OF MSDH

a. MSDH shall provide Business Associate with the Notice of Privacy Practices that MSDH produces in accordance with 45 C.F.R. § 164.520, as well as any changes to such Notice of Privacy Practices, upon request.

b. MSDH shall notify Business Associate of any limitation(s) in its Notice of Privacy Practices to the extent that such limitation may affect Business Associate's Use or Disclosure of PHI.

c. MSDH shall notify Business Associate of any changes in, or revocation of, permission by an Individual to Use or Disclose PHI, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI.

d. MSDH shall notify Business Associate of any restriction to the Use or Disclosure of PHI that MSDH has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's Use or Disclosure of PHI.

e. Permissible Requests by MSDH: MSDH shall not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the Privacy Rule if done by MSDH, except as provided for in Section (IV) of this Agreement.

VI TERM AND TERMINATION

a. Term. For any new Underlying Agreement(s) entered into between MSDH and Business Associate, the effective date of this Agreement is the effective date of the Underlying Agreement(s) entered into between MSDH and Business Associate. For any ongoing Underlying Agreement(s) entered into between MSDH and Business Associate, the effective date of this Agreement is the date first herein written. This Agreement shall terminate when all of the PHI provided by MSDH to Business Associate or created or received by Business Associate on behalf of MSDH, is destroyed or returned to MSDH, 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. Termination of this Agreement shall automatically terminate the Underlying Agreement(s).

b. Termination for Cause. Upon MSDH's knowledge of a material Violation by Business Associate, MSDH shall, at its discretion, either:

i. provide an opportunity for Business Associate to cure or end the Violation within a time specified by MSDH, after which MSDH may in its discretion terminate this Agreement and the Underlying Agreement(s) if Business Associate does not cure or end the Violation within the time specified by MSDH; or

ii. immediately terminate this Agreement and the associated Underlying Agreement(s) if Business Associate has broken a material term of this Agreement and cure is not possible.

c. Effect of Termination.

i. Upon termination of this Agreement and the Underlying Agreement(s) for any reason, Business Associate shall return or destroy all PHI received from or created or received by Business Associate on behalf of, MSDH in accordance with State and Federal retention guidelines. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

ii. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to MSDH notification of the conditions that make return or destruction infeasible. Upon notification in writing that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further Uses and Disclosures to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VII. MISCELLANEOUS

a. Statutory and Regulatory References. A reference in this Agreement to a section in HIPAA, its implementing regulations, or other applicable law means the section as in effect or as amended, and for which compliance is required.

b. Amendments/Changes in Law.

i. General. Modifications or amendments to this Agreement may be made upon mutual agreement of the Parties, in writing signed by the Parties hereto and approved as required by law. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in this Agreement. Such modifications or amendments signed by the Parties shall be attached to and become part of this Agreement.

ii. Amendments as a Result of Changes in the Law. The Parties agree to take such action as is necessary to amend this Agreement as is necessary to effectively comply with any subsequent changes or clarifications of statutes, regulations, or rules related to this Agreement. The Parties further agree to take such action as is necessary to comply with the requirements of HIPAA, its implementing regulations, and other applicable law relating to the security and privacy of PHI.

iii. Procedure for Implementing Amendments as a Result of Changes in Law. In the event that there are subsequent changes or clarifications of statutes, regulations or rules relating to this Agreement, or the Parties' compliance with the laws referenced in Section (VII)(b) of this Agreement necessitates an amendment, the requesting party shall notify the other party of any actions it reasonably deems are necessary to comply with such changes or to ensure compliance, and the Parties promptly shall take such actions. In the event that there shall be a change in the federal or state laws, rules or regulations, or any interpretation of any such law, rule, regulation, or general instructions which may render any of the material terms of this Agreement unlawful or unenforceable, or materially affects the financial arrangement contained in this Agreement, the Parties may, by providing advanced written notice, propose an amendment to this Agreement addressing such issues.

c. Survival. The respective rights and obligations of Business Associate provided for in Sections (III)(j) and (VI)(c) of this Agreement shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit MSDH to comply with HIPAA, its implementing regulations, and other applicable law relating to the security and privacy of PHI.

e. Indemnification. To the fullest extent allowed by law, Business Associate shall indemnify, defend, save and hold harmless, protect, and exonerate MSDH, its employees, agents, and representatives, and the State of Mississippi from and against all claims, demands, liabilities, suits, actions, damages, losses, and costs of every kind and nature whatsoever including, without limitation, court costs, investigative fees and expenses, and attorney's fees, arising out of or caused by Business Associate and/or its partners, principals, agents, and employees in the performance of or failure to perform this Agreement. In MSDH's sole discretion, Business Associate may be allowed to control the defense of any such claim, suit, etc. In the event Business Associate defends said claim, suit, etc., Business Associate shall utilize legal counsel acceptable to MSDH. Business Associate shall be solely responsible for all costs and/or expenses associated with such defense, and MSDH shall be entitled to participate in said defense. Business Associate shall not settle any claim, suit, etc. without MSDH's concurrence, which MSDH shall not unreasonably withhold.

MSDH's liability, as an entity of the State of Mississippi, is determined and controlled in accordance with Mississippi Code Annotated § 11-46-1 et seq., including all defenses and exceptions contained therein. Nothing in this Agreement shall have the effect of changing or altering the liability or of eliminating any defense available to the State under statute.

f. Disclaimer. MSDH makes no warranty or representation that compliance by Business Associate with this Agreement, HIPAA, its implementing regulations, or other applicable law will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized Use or Disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

g. Notices. Any notice from one party to the other under this Agreement shall be in writing and may be either personally delivered, emailed, or sent by registered or certified mail in the United States Postal Service, Return Receipt Requested, postage prepaid, addressed to each party at the addresses which follow or to such other addresses provided for in this Agreement or as the Parties may hereinafter designate in writing:

MSDH: (Covered Entity)

Privacy Officer
Mississippi State Department of Health
570 East Woodrow Wilson
Suite O-150
P. O. Box 1700
Jackson, MS 39215
601-576-7874

IT Security Officer
Mississippi State Department of Health
570 East Woodrow Wilson
Suite O-450
P.O. Box 1700
Jackson, MS 39215
601-576-7821

Business Associate:

Name of Business: _____

Attn: _____

Title: _____

Address: _____

Phone: _____

Email: _____

Any such notice shall be deemed to have been given as of the date transmitted.

h. Severability. It is understood and agreed by the Parties hereto that if any part, term, or provision of this Agreement is by the courts or other judicial body held to be illegal or in conflict with any law of the State of Mississippi or any federal law, the validity of the remaining portions or provisions shall not be affected and the obligations of the parties shall be construed in full force as if this Agreement did not contain that particular part, term, or provision held to be invalid.

i. Applicable Law. This Agreement shall be construed broadly to implement and comply with the requirements relating to HIPAA and its implementing regulations. All other aspects of this Agreement shall be governed by and construed in accordance with the laws of the State of Mississippi, excluding its conflicts of laws provisions, and any litigation with respect thereto shall be brought in the courts of the State. Business Associate shall comply with applicable federal, state, and local laws, regulations, policies, and procedures as now existing and as may be amended or modified. Where provisions of this Agreement differ from those mandated by such laws and regulations, but are nonetheless permitted by such laws and regulations, the provisions of this Agreement shall control.

j. Non-Assignment and Subcontracting. Business Associate shall not assign, subcontract, or otherwise transfer this Agreement, in whole or in part, without the prior written consent of MSDH. Any attempted assignment or transfer of its obligations without such consent shall be null and void. No such approval by MSDH of any subcontract shall be deemed in any way to provide for the incurrence of any obligation of MSDH in addition to the total compensation agreed upon in this Agreement. Subcontracts shall be subject to the terms and conditions of this Agreement and to any conditions of approval that MSDH may deem necessary. Subject to the foregoing, this Agreement shall be binding upon the respective successors and assigns of the parties. MSDH may assign its rights and obligations under this Agreement to any successor or affiliated entity.

k. Entire Agreement. This Agreement contains the entire agreement between the Parties and supersedes all prior discussions, instructions, directions, understandings, negotiations, agreements, and services for like services.

l. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and their respective successors, heirs, or permitted assigns, any rights, remedies, obligations, or liabilities whatsoever.

m. Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself and any workforce members, contractors, subcontractors, representatives, agents, affiliates, or subsidiaries assisting Business Associate in the fulfillment of its obligations under this Agreement, available to MSDH, at no cost to MSDH, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against MSDH, its directors, officers, or any other workforce member based upon claimed Violation of HIPAA, its implementing regulations, or other applicable law, except where Business Associate or its workforce members, contractors, subcontractors, representatives, agents, affiliates, or subsidiaries are a named adverse party.