HIPAA Policy for ITS Operations
Notice of Approval

Mississippi Department of Information Technology Services	**Doc Ref Number:** ITS-PSG-3001	
	Title: HIPAA Policy for ITS Operations	
	Document Type: ITS Agency	
	Domain: Security | Compliance	**Status:** Approved
	Effective Date: 09-11-2017	**Revision Date:** 09-11-2017

Notice is hereby given, that the above specified document meets the requirements of the Mississippi Department of Information Technology Services Policies, Standards and Guidelines Program, defined in ESW-PSG-1001. Thereby warranting approval for implementation, effective immediately.

Executive Director
Mississippi Department of
Information Technology Services

September 11, 2017
Date of Signature

Mississippi Department of Information Technology Services	**Doc Ref Number:** ITS-PSG-3001	
	Title: HIPAA Policy for ITS Operations	
	Document Type: ITS Operational	**Page:** 1 of 9
	Domain: Security | Compliance	**Status:** Approved
	Effective Date: 09-11-2017	**Revision Date:** 09-11-2017

1. AUTHORITY

The Mississippi Department of Information Technology Services (ITS) shall issue recommended strategies and goals for the effective and efficient use of information technology and services in state government (§ 25-53-29(2)). Additionally, ITS shall publish written planning guides, policies and procedures for use by agencies and institutions in planning future electronic information service systems (§ 25-53-29(1) (b)).

2. PURPOSE

This HIPAA (Health Insurance Portability and Accountability Act) Policy for ITS Operations provides guidance to the Mississippi Department of Information Technology Services (ITS) concerning the safeguards to securely store and transmit partner agency's electronic protected health information (ePHI) data. ITS is committed to protecting the electronic files, media, databases, and data maintained by the agency. ITS must implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive information when the unauthorized use of such information is likely to result in substantial harm or inconvenience to the State. This HIPAA policy provides the framework for ITS leadership to ensure the confidentiality and security of all electronic files, media, databases and data within the agency's operational divisions.

3. SCOPE

This HIPAA Policy for ITS Operations applies to ITS staff, defined as full-time, part-time, temporary, contract employees, persons who are employed by contractors or subcontractors of ITS, and visitors that may come into contact with HIPAA data in the performance of their duties. Individuals with permanent physical access authorization credentials are not considered visitors.

4. POLICY

4.1 ITS shall designate a HIPAA Privacy Officer to be responsible for the development and implementation of the policies and procedures necessary for HIPAA compliance.

4.2 ITS shall implement reasonable physical security measures at the State Data Center facilities to:

4.2.2 Ensure the security of the facilities
4.2.3 Protect against anticipated threats or hazards to the facilities

4.2.4 Protect against unauthorized access to the facilities

4.3 ITS shall implement reasonable security measures on the underlying infrastructure housed in the State Data Center required provisioning computing resources to:

4.3.2 Ensure the security of the underlying infrastructure
4.3.3 Protect against anticipated threats to the underlying infrastructure
4.3.4 Protect against unauthorized access to the underlying infrastructure
4.3.5 Isolate partner agency computing resources hosted in the State Data Center(s) to the proper network segment

4.4 ITS shall work with any authorized business partners providing services for storing, processing, or transmitting ePHI data to strive towards compliance to all applicable HIPAA policy requirements.

4.5 ITS shall work with partner agencies to identify all systems that receive, maintain, or transmit ePHI.

4.6 ITS shall work with partner agencies to strive toward compliance in all applicable policies such as the Statewide Enterprise Security Policy, ITS Security Policy and HIPAA requirements for all systems that receive, maintain, or transmit ePHI.

4.7 ITS shall work with partner agencies regarding any ePHI data that ITS Operations has administrative access to ensure the confidentiality, integrity, and availability ITS Operation's Divisions receives, maintains, or transmits of ePHI data.

4.8 ITS shall protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.

4.9 ITS shall ensure compliance by the entire ITS staff through awareness and training.

4.10 ITS shall work with partner agencies to initiate Business Associate Agreements with updated Health Information Technology for Economic and Clinical Health Act (HITECH) language with business associates as needed.

4.8.1 Business Associate Agreements
The HIPAA Rules have extended applicability of the rules designed to protect data from unauthorized use or release to business associates. These rules include HIPAA Privacy, Security, Breach Notification, and Enforcement Rules. Therefore, it will be the responsibility of ITS to attempt to negotiate appropriate HIPAA

Business Associate Agreements with Business Associates that might access protected health information. ITS will keep records to indicate information concerning the negotiation of these contracts. These records should include such information as when the agreement was sent to the business associate, date the agreement was received from the business associate and entries as to additional contacts as well as the status of any negotiation with the business associate. It should be remembered by ITS staff that by federal statute business associates have specific obligations whether there is a business associate agreement in place or not.

5. STANDARD

In accordance with section 4.8 of this policy ITS should use the language and format of the Business Associate Agreement Template found in Attachment A as the standard when initiating Business Associate Agreements with state agencies or other covered entities.

6. ATTACHMENTS

ATTACHMENT A: Business Associate Agreement Template

ATTACHMENT A: Business Associate Agreement Template

BUSINESS ASSOCIATE AGREEMENT BETWEEN MISSISSIPPI DEPARTMENT OF INFORMATION TECHNOLOGY SERVICES AND {STATE AGENCY}

This Business Associate Agreement ("Agreement") is entered into as of the date it is last signed below ("Effective Date") by and between the Mississippi Department of Information Technology Services ("Business Associate") and the ***{STATE AGENCY}*** ("Covered Entity"), hereinafter referred to individually as a "Party" and collectively, the "Parties". This Agreement supersedes any previously executed Business Associate Agreement between the Parties.

WHEREAS, Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as modified by the Health Information Technology for Economic and Clinical Health Act, known collectively as "the Administrative Simplification provisions," direct the Department of Health and Human Services to develop standards to protect the security, confidentiality and integrity of health information; and

WHEREAS, pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services has issued regulations at 45 CFR Parts 160 and 164, as the same may be amended from time to time (the "HIPAA Security and Privacy Rule"); and

WHEREAS, the Parties wish to enter into or have entered into an arrangement whereby Business Associate will provide certain services to Covered Entity, and, pursuant to such arrangement, Business Associate may be considered a "business associate" of Covered Entity as defined in the HIPAA Security and Privacy Rule (the agreement evidencing such arrangement is hereinafter referred to as "Inter-Agency Agreement"); and

WHEREAS, Business Associate may have access to Protected Health Information (as defined below) in fulfilling its responsibilities under such Inter-Agency Agreement;

THEREFORE, in consideration of the Parties' continuing obligations under the Inter-Agency Agreement, compliance with the HIPAA Security and Privacy Rule, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement in order to address the requirements of the HIPAA Security and Privacy Rule and to protect the interests of both Parties.

ARTICLE I DEFINITIONS

Except as otherwise defined herein, any and all capitalized terms in this Agreement shall have the definitions set forth in the HIPAA Security and Privacy Rule. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Security and Privacy Rule, as amended, the HIPAA Security and Privacy Rule shall control. Where provisions of this Agreement are different from those mandated in the HIPAA Security and Privacy Rule, but are nonetheless permitted by the HIPAA Security and Privacy Rule, the provisions of this Agreement shall control.

1. **"Agreement"** shall mean this Business Associate Agreement.
2. **"Breach"** shall mean the acquisition, access, Use or Disclosure of Protected Health Information ("PHI"), PII, and ***{STATE AGENCY}*** Confidential Information in a manner not permitted by the HIPAA Security and Privacy Rule which compromises the security or privacy of the PHI, and subject to the exceptions set forth in 45 CFR 164.402.
3. **"Business Associate"** shall mean the Mississippi Department of Information Technology Services, including all employees, contractors, subcontractors, representatives, agents, successors and assigns.
4. **"*{STATE AGENCY}* Confidential Information"** shall mean:
   i. all data that is collected, stored, processed, or generated by or on behalf of ***{STATE AGENCY}***;
   ii. any information from which an individual may be uniquely identified, including, without limitation, an individual's name, address, telephone number, social security number, birth date, account numbers, and healthcare information;

iii. all data provided to ***{STATE AGENCY}*** by the Social Security Administration (SSA);

iv. any reference to the identity, physical location, financial information, and medical services of a ***{STATE AGENCY}*** provider and any other DOM provider information protected by federal and Mississippi law; and,

v. any or all other sensitive, confidential, or proprietary information that has been classified, marked, or announced as sensitive, confidential, or proprietary, or which, because of the circumstances of disclosure or the nature of the information itself, would be reasonably understood to be sensitive, confidential, or proprietary.

5. **"Covered Entity"** shall mean the Mississippi ***{STATE AGENCY}***.

6. **"Effective Date"** shall mean the date this Agreement is last signed by all Parties.

7. **"HIPAA"** shall mean the Health Insurance Portability and Accountability Act of 1996 as may be now or hereafter amended or modified.

8. **"Inter-Agency Agreement"** shall mean the arrangement whereby Business Associate will provide certain services to Covered Entity.

9. **"Personally Identifiable Information (PII)"** which is defined by the United States Government Accountability Office (GAO) as, "any information about an individual maintained by an agency, including, 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, any other information that is linked or linkable to an individual, such as a medical, education, financial, and employment information."

10. **"Protected Health Information" or "PHI"** shall have the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. Protected Health Information includes without limitation "Electronic Protected Health Information" as defined herein.

11. **"Electronic Protected Health Information"** shall mean Protected Health Information that is transmitted by electronic media (as defined in the HIPAA Security & Privacy Rule) or maintained in electronic media.

ARTICLE II OBLIGATIONS & ACTIVITIES OF BUSINESS ASSOCIATE

1. **Security & Privacy Rules**: Business Associate agrees to comply with the HIPAA Security and Privacy Rules that are applicable to a "business associate" and with the Covered Entity's privacy and security policies.

2. **Protected Health Information**: Business Associate agrees to not Use or Disclose PHI other than as permitted or requested by this Agreement or as required by law.

3. **Safeguards**: Business Associate agrees to use appropriate safeguards and comply, where applicable, with the Security Rule, to prevent Use or Disclosure of the PHI other than as provided for by this Agreement.

4. **Mitigation**: Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in Violation of the requirements of this Agreement.

5. **Breach Notification**: Business Associate agreed to promptly notify Covered Entity of a Breach of Unsecured PHI by Business Associate or its subcontractors or any of their employees or agents of which it becomes aware.

6. **Security Incident Reporting**: Business Associate agrees to notify Covered Entity of any Security Incident of which it becomes aware.

7. **Agents**: Business Associate agrees to ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such information.

8. **Access**: Business Associate agrees to provide reasonable access, at the request of Covered Entity, to PHI in a Designated Record Set to Covered Entity, or as directed by Covered Entity, to an Individual in order to meet the requirements of 45 CFR 164.524 and the HIPAA Security & Privacy Rules.

9. **Amendments**: Business Associate agrees to make any amendments to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR 164.526.

10. **Audit**: Business Associate agrees to make internal practices, books, and records, including PHI and policies and procedures relating to the Use and Disclosure of PHI, available to the Secretary, in a time and manner mutually agreed to by Business Associate and the Secretary, for purposes of the

Secretary determining Covered Entity's or Business Associate's compliance with the HIPAA Security and Privacy Rules.

11. **Accounting**: Business Associate agrees to document such Disclosures of PHI 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 PHI in accordance with 45 CFR 164.528. Business Associate agrees to provide to Covered Entity and/or an Individual (as requested) within thirty (30) calendar days of receipt of a written request, such information as necessary to permit Covered Entity to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR 164.528.

12. **Restrict Use/Disclosure**: Business Associate agrees to restrict the Use or Disclosure of PHI as required by 42 U.S.C. 17935(a) and 45 CFR 164.522, as requested by Covered Entity or an Individual. Covered Entity will notify Business Associate in writing of the restriction that Business Associate must follow and will promptly notify Business Associate in writing of the termination of any such restriction and instruct Business Associate whether any PHI will remain restricted.

13. **No Sale of PHI**: Business Associate agrees not to directly or indirectly receive remuneration in exchange for PHI or otherwise engage in a Sale of PHI unless Business Associate obtains Covered Entity's prior written approval and the Individual has provided his or her authorization and written permission, including a statement that the disclosure will result in remuneration to Business Associate and a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the Individual's PHI, in accordance with the HIPAA Security and Privacy Rules.

14. **Marketing Limits**: Business Associate agrees not to make or cause to be made any communication about a product or service or otherwise engage in Marketing that is prohibited by 42 U.S.C. 17936 or does not meet the requirements of the HIPAA Security and Privacy Rules, including the requirement to obtain authorization to comply with 45 CFR 164.508.

15. **Genetic Information Restrictions**: Business Associate agrees not to Use or Disclose Genetic Information for underwriting purposes in violation of the HIPAA Security and Privacy Rules.

16. **HITECH Act**: Business Associate agrees that 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.

ARTICLE III PERMITTED USES & DISCLOSURES

1. 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, Covered Entity as specified in the Inter-Agency Agreement, provided that such Use or Disclosure would not Violate the HIPAA Security and Privacy Rules if done by Covered Entity.

2. Business Associate is authorized to de-identify PHI and Use or Disclose de-identified PHI in accordance with 45 CFR 164.514(a)-(c). Any Use or Disclosure of PHI by Business Associate shall be limited to a Limited Data Set or the Minimum Necessary to accomplish the intended purpose of such Use or Disclosure, or otherwise comply with guidance on "minimum necessary" as promulgated by the Secretary in accordance with section 13405(b) of the HITECH Act, as codified at 42 U.S.C. section 17935(b).

3. 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 Inter-Agency Agreement entered into between Covered Entity and Business Associate.

4. 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, or Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will remain confidential and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.

5. Business Associate may Use PHI to provide Data Aggregation services to Covered Entity upon Covered Entity's request as permitted by 45 CFR 164.504(e)(2)(i)(B).

6. Business Associate may Use PHI to report violations of law to appropriate Federal and state authorities, consistent with 45 CFR 164.502(j)(1).

ARTICLE IV OBLIGATIONS OF COVERED ENTITY

1. Covered Entity shall provide Business Associate with the Notice of Privacy Practices that Covered Entity produces in accordance with 45 C.F.R. § 164.520, as well as any changes to such Notice of Privacy Practices.
2. Covered Entity shall notify affected Individuals, the Secretary, or the media, as applicable, upon a Breach of Unsecured Protected Health Information in accordance with the HIPAA Security and Privacy Rules.
3. Covered Entity shall notify Business Associate of any limitations in its Notice of Privacy Practices to the extent that such limitation may affect Business Associate's Use or Disclosure of PHI.
4. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to Use or Disclose PHI, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI.
5. Covered Entity shall notify Business Associate of any restriction to the Use or Disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's Use or Disclosure of PHI.
6. Except as provided above regarding data aggregation and management and administrative activities of Business Associate, Covered Entity 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 Covered Entity.
7. For all data and computing resources hosted in the State Data Center that Covered Entity has administrative access to, Covered Entity is solely responsible for properly configuring and implementing security measures to maintain security and protection.

8. For all data and computing resources hosted in the State Data Center that Covered Entity has administrative access to, Covered Entity is required to adhere to the State Enterprise Security Policy (ESP), using the ESP as minimum security requirements when implementing their individual agency IT security policies, plans, and procedures.

9. For all data and computing resources hosted in the State Data Center that Covered Entity has administrative access to, Covered Entity is solely responsible for identifying any guidelines, regulations, or laws (Federal, State, or Local) outside of the ESP that they are required to meet. Furthermore, Covered Entity is solely responsible for maintaining compliance with said guidelines, regulations, or laws. Any requirement of a guideline, regulation, or law not detailed in this Agreement that requires Business Associate's involvement for compliance will not be the responsibility of Business Associate.

10. For all data and computing resources hosted in the State Data Center for Covered Entity, Covered Entity must disclose to Business Associate if any of the resources will be used now or in the future to store or process Personally Identifiable Information (PII) or other sensitive/confidential information. Covered Entity must also disclose to Business Associate if any resources will be used now or in the future to store or process data covered under guidelines, regulations, or laws (Federal, State, Local) outside of the ESP. The guidelines, regulations, or laws may include, but are not limited to:

    - Health Insurance Portability and Accountability Act of 1996 (HIPPA)
    - Family Educational Rights and Privacy Act (FERPA)
    - Payment Card Industry Data Security Standards (PCI/DSS)
    - Tax Information Security Guidelines for Federal, State, and Local Agencies
    - Children's Internet Protection Act (CIPA)
    - Federal Information Security Management Act of 2002 (FISMA)
    - Other.

11. For all data and computing resources hosted in the State Data Center for Covered Entity, Covered Entity is responsible for End Users' use of all data and computing resources. Covered Entity will ensure that End Users comply with customer obligations under this Agreement and that the terms of the Agreement with each End User are consistent with this Agreement. Additionally, if Covered Entity becomes aware of any violation of its obligations under this Agreement, by an End User, Covered Entity will immediately terminate such End User's access to all data and computing resources.

12. Covered Entity is solely responsible for encrypting all PHI stored in or transmitted in accordance with the State of Mississippi's Enterprise Security Policy and in accordance with the Secretary of HHS's Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

13. Covered Entity is solely responsible for ensuring that PHI transmitted is encrypted end-to-end. Any PHI that is in transit must be encrypted at all times, and may not be decrypted by ITS.

14. Covered Entity is solely responsible for ensuring that all compute instances process, storing, or transmitting PHI are Dedicated Instances.

15. Covered Entity must not agree to any restriction requests or place any restrictions in any notice of privacy and security practices that would cause ITS to violate this agreement or any applicable law.

16. Covered Entity must not request or cause ITS to make a Use or Disclosure of PHI in a manner that does not comply with HIPAA or this agreement.

17. Covered Entity's compliance with all terms of this Agreement are subject to review by ITS.

ARTICLE V TERM AND TERMINATION

1. **Term**: This Agreement shall begin on the Effective Date and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or if it is not feasible to return or destroy the PHI, until protections are extended to such information in accordance with the termination provisions in this section.

2. **Termination For Cause**: Upon Covered Entity's knowledge of a material Breach or Violation by Business Associate, Covered Entity shall, at its discretion, either: (a) provide an opportunity for Business Associate to cure the Breach or end the Violation and terminate this Agreement and the associated Inter-Agency Agreement, if Business Associate does not cure the Breach or end the Violation within the time specified by Covered Entity, or (b) immediately terminate this Agreement and the associated Inter-Agency Agreement if Business Associate has Breached a material term of this Agreement and cure is not possible.

3. **Effect of Termination**:

(a) Except as provided in paragraph (b) of this Article V(3), upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from, or created or received by Business Associate on behalf of Covered Entity in accordance with State and Federal retention guidelines. This provision shall apply to PHI that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

(b) In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide Covered Entity notification of the conditions that make return or destruction infeasible. Upon notification in writing that return or destruction of PHI is not feasible, 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.

ARTICLE VI MISCELLANEOUS

1. **Statutory & Regulatory References**: A reference in this Agreement to a section in HIPAA, the HITECH Act, their implementing regulations, or other applicable law means the section as in effect or as amended, and for which compliance is required.

2. **Amendments**: This Agreement may be modified only by written agreement signed by the Parties hereto, and any attempt at oral modification shall be void and of no effect. The Parties agree to take such action 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 laws relating to the security and privacy of PHI.

3. **Interpretation**: Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with HIPAA, its implementing regulations, and other applicable law relating to the security and privacy of PHI.
4. **Severability**: In the event any provision of this Agreement is held to be unenforceable for any reason, the unenforceability thereof shall not affect the remainder of this Agreement, which shall remain in full force and effect and enforceable in accordance with its terms.
5. **Notices**: Any notice required or permitted to be given under this Agreement shall be in writing and personally delivered or sent by electronic means provided that the original of such notice is sent by certified United States mail, postage prepaid, return receipt requested, or overnight courier with signed receipt, to the party to whom the notice should be given at their business address listed herein. Business Associate's address for notice is: Craig P. Orgeron, Ph.D., Executive Director, Mississippi Department of Information Technology Services, 3771 Eastwood Drive, Jackson, Mississippi 39211. Covered Entity's address for notice is: ***{STATE AGENCY}***
6. **Governing Law**: This Agreement shall be construed broadly to implement and comply with the requirements relating to HIPAA, its implementing regulations, and other applicable law relating to the security and privacy of PHI. All other aspects of this Agreement shall be governed under the laws of the State of Mississippi. 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.
7. **Assignment**: Neither Party may assign or otherwise transfer this Agreement or its obligations hereunder without the prior written consent of the other Party. The rights and obligations of the Parties will inure to the benefit of, will be binding upon, and will be enforceable by the Parties and their lawful successors, authorized assigns, and representatives.
8. **Reporting:** For all reporting obligations under this agreement, ITS and {STATE AGENCY} acknowledge that, because ITS does not know the nature of PHI contained in any of {STATE AGENCY}'s systems, it will not be possible for ITS to provide information about the identities of the individuals who may have been affected, or a description of the type of information that may have been subject to a Security Incident, Impermissible Use or Disclosure, or Breach.

For the faithful performance of the terms of this Agreement, the Parties hereto have caused this Agreement to be executed by their undersigned authorized representatives.

Business Associate:
Mississippi Department of Information Technology Services

By:_____
Authorized Signature

Printed Name: Craig P. Orgeron, Ph.D.

Title: Executive Director

Date:_____

Covered Entity:
{STATE AGENCY}

By:_____
Authorized Signature

Printed Name: *{STATE AGENCY}*

Title: Executive Director

Date:_____