

BUSINESS ASSOCIATE AGREEMENT
And
MEMORANDUM OF UNDERSTANDING
Between
DEPARTMENT OF BUDGET AND MANAGEMENT
And
DEPARTMENT OF INFORMATION TECHNOLOGY

This Intergovernmental Memorandum of Understanding, also known as a Business Associate Agreement, is effective this 1st of July, 2008 by and between the Department of Budget and Management, (“DBM”) and the Department of Information Technology (“DoIT”).

- 1. Definitions**
- 1.1** “ASM” means Application Systems Management, a unit of DoIT.
- 1.2** “Benefits Administration System” or “BAS” means the relational database and its related enhancements, modules and Interactive Voice Response System (IVR) used by DBM to support Program related functions,
- 1.3** “Business Associate Agreement” or “BAA” means this Agreement regarding the use, disclosure, and protection of PHI and electronic PHI and DoIT’s information technology related support of DBM’s activities in connection with the Program.
- 1.4** “Covered Entity” means a covered entity as defined by 45 CFR §160.103.
- 1.5** “DBM” means the Department of Budget and Management.
- 1.6** “Designated Record Set” means a group of records maintained by or for the DoIT/ASM that includes (i) the medical records and billing records about individuals enrolled in the Program, (ii) the enrollment, payment, claims adjudication, and case or medical management record systems related to individuals enrolled in the Program or (iii) records used, in whole or in part, to make decisions about individuals enrolled in the Program. Records and data stored in the Benefits Administration System may be a Designated Record Set.
- 1.7** “DHHS” means the United States Department of Health and Human Services and includes the Secretary of DHHS.
- 1.8** “Disclosure” or “Disclose” means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
- 1.9** “DoIT” means the Department of Information Technology,

- 1.10 “EBD” means the Employee Benefits Division, a unit of OPSB within DBM.
- 1.11 “HIPAA Privacy Regulation” means the regulations regarding standards for privacy of individually identifiable health information implemented by DHHS at 45 CFR Parts 160 and part 164, pursuant to the Health Insurance Portability and Accountability Act of 1996, as these regulations may be amended.
- 1.12 “OPSB” means the Office of Personnel Services and Benefits, a unit of DBM.
- 1.13 “PHI” means protected health information, as that phrase is defined in 45 CFR §164.501, limited for purposes of this Business Associate Agreement to the information created by, received by or in the control, custody or possession of DoIT in the administration of the Program. All records in the Benefits Administration System and Interactive Voice Response system used in the administration of the Program are PHI.
- 1.14 “Program” means the State Employees and Retirees Health and Welfare Benefits Program, the group health arrangement through which various health benefits plans are offered to State employees, retirees and their dependents. The Program is administered by DBM.
- 1.15 “Security Incident” means any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system in which electronic PHI is maintained, created, transmitted, or received.
- 1.16 “Use” means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

2. Scope and Term

- 2.1 Any ambiguity in this Business Associate Agreement shall be resolved to permit the parties to comply with the HIPAA Privacy Regulation in connection with access to, use and disclosure of PHI, including enrollment and payment information, gathered in administration of the Program and support of that administration.
- 2.2 This BAA shall be effective from its execution through the term and duration of any period during which DoIT or ASM provide information technology support to the DBM that results in or requires access by DoIT/ASM to PHI.
- 2.3 DBM and DoIT may terminate this BAA by mutual agreement, provided that to the extent PHI, in whatever format, remains in the custody, control or possession of DoIT, adequate arrangements are made to protect the security and confidentiality of such PHI.

- 2.4 The parties agree to take such action to amend this Business Associate Agreement from time to time as is necessary for each party to comply with the requirements of the HIPAA Privacy Regulation.
- a. Neither party will unilaterally modify an obligation under this BAA without consultation and mutual agreement.
 - b. No amendment or modification to terms of this BAA is binding unless it is in writing and signed by the secretaries of both departments.
- 2.5 Nothing express or implied in this Business Associate Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assigns of the parties, any rights, remedies, obligations or liabilities whatsoever.
- 2.6 No new funding will transfer between the departments for the services outlined in this BAA.
- 2.7 Both DBM and DoIT will make good faith efforts to resolve any disagreements concerning any of the provisions of this BAA. In the event that officials and employees of the departments involved in implementing this BAA are unable to resolve a disagreement despite such good faith efforts, the disagreement shall be referred to and jointly decided by the Secretary of Budget and Management and the Secretary of Information Technology.
- 3. Obligations and Activities of the DoIT/ASM**
- 3.1 DoIT and ASM shall not Use or Disclose PHI except as permitted by this Business Associate Agreement.
- 3.2 DoIT, primarily through ASM, will provide administration, management, operational and maintenance support services for all OPSB Program and employee benefits systems and processes, as detailed herein and in the Memorandum of Understanding executed between the Departments and effective July 1, 2008.
- 3.3 DoIT/ASM shall implement and use appropriate and reasonable administrative, physical and technical safeguards to maintain the security of and to prevent use or disclosure of PHI other than (a) as provided in this BAA, (b) permitted by the HIPAA Privacy Regulation for a Covered Entity, and (c) permitted by the Medical Records Act. In the event that the HIPAA Privacy Regulation and the Medical Records Act conflict regarding the degree of protection provided for PHI, DoIT/ASM shall comply with the more restrictive protection requirements.

- 3.4 DoIT/ASM shall report to the DBM any use or disclosure of PHI that is not permitted by this Business Associate Agreement within 10 days of when DoIT/ASM becomes aware of such use or disclosure.
- 3.5 DoIT/ASM shall use reasonable efforts to mitigate the effect of any use or disclosure of PHI known to DoIT/ASM that is not permitted by this Business Associate Agreement.
- 3.6 DoIT/ASM shall ensure that any agents, including contractors and subcontractors, to whom it provides PHI agree to the same restrictions and conditions that apply to DoIT/ASM with respect to such PHI. DoIT/ASM shall provide notice to DBM of any access provided to DoIT/ASM contractors or subcontractors to PHI, whether in electronic or other format.
- 3.7 DoIT/ASM shall maintain PHI and make available to DBM any PHI in a Designated Record Set relating to an individual upon request of DBM to permit DBM to comply with an individual's request pursuant to 45 CFR §164.524.
- 3.8 DoIT/ASM shall make available for amendment and amend PHI in a Designated Record Set it holds at the request of the DBM.
- 3.9 DoIT/ASM shall document and track disclosures, including sufficient information as would be required by DBM to respond to a request for an accounting in accordance with 45 CFR §164.528, and provide an accounting of Disclosures of PHI to DBM upon request. Any disclosure or use of PHI by DoIT/ASM shall be noted.
- 3.10 DoIT/ASM shall make internal practices, books and records, including privacy and confidentiality policies and procedures and PHI, available and DHHS, for purposes of determining whether DBM is compliant with the HIPAA Privacy Regulation in the administration of the Program.
- 3.11 Upon termination of the MOU and provision of information technology support services by DoIT/ASM for DBM and the Employee Benefits Division, DoIT shall return all copies of PHI, whether electronic or in other form, to DBM; if such return is not feasible, DoIT shall extend the protections of this Business Associate Agreement to the PHI it retains in its possession, custody and control for so long as the DoIT/ASM maintains the PHI. Such records may be destroyed after six years with the approval of DBM.
- 3.12 DoIT/ASM shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that DoIT/ASM creates, receives, maintains, or transmits in performing DoIT/ASM's obligations under the MOU.

3.13 DoIT/ASM shall ensure that any agent to whom it provides electronic PHI agrees to implement reasonable and appropriate safeguards to protect such electronic PHI.

3.14 DoIT/ASM shall report to the DBM any Security Incident in connection with the DoIT/ASM's systems that contain, house, or have access to PHI, including but not limited to any back-up copies of data in the Benefits Administration System. In the event of a Security Incident, DoIT/ASM shall take reasonable and appropriate steps in mitigation or remediation of the security incident and shall notify the DBM of such steps.

4. Permitted Uses and Disclosures by DoIT/ASM

4.1 DoIT/ASM shall use and disclose the minimum amount of PHI necessary to provide the services required by the MOU, as amended from time to time. Such services include information technology support of the DBM Benefits Administration System, the Interactive Voice Response System, and the various information technology needs of the DBM Employee Benefits Division in the administration of the Program.

4.2 DoIT/ASM may disclose PHI as required by law in compliance with 45 CFR §164.512.

4.3 DoIT/ASM may use and disclose PHI for the proper management and administration of the Maintenance Agreement or to carry out its legal responsibilities as permitted by 45 CFR §164.504(e)(4), provided that: (a) such uses and disclosures would be permitted by the HIPAA Privacy Regulation if DoIT/ASM were a Covered Entity regulated by the HIPAA Privacy Regulation and (b) DoIT/ASM obtains reasonable assurances from the person, agency, or entity to which such Disclosures are made that all PHI will remain confidential and used or disclosed further only as required by law, for the purposes of the disclosure by DoIT/ASM, and the person, agent or entity notifies DoIT/ASM of any instances in which the confidentiality of the PHI has been breached.


4.4 DoIT/ASM may use or disclose PHI to report violations of the law to appropriate State and federal authorities consistent with 45 CFR §164.502(j).

5. Obligations of the DBM

5.1 DBM shall provide the DoIT/ASM with the notice of privacy practices that the DBM produces in accordance with 45 C.F.R. § 164.520, as well as any changes to that notice.

5.2 DBM shall not request the DoIT/ASM to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Regulation if done by the DBM.

We hereby agree to operate pursuant to the understanding provided for above.



T. Eloise Foster
Secretary
Department of Budget and Management



Elliot Schlanger
Secretary
Department of Information Technology