DATA USE AGREEMENT

Attachment D

Notification of Breach

I. Definitions. All terms used in this Attachment D, but not otherwise defined, shall have the same meanings as assigned to those terms in the Data Use Agreement ("Agreement") to which this Attachment D is incorporated.

II. Breaches and Security Incidents. During the term of the Agreement, User agrees to implement reasonable systems for the discovery and prompt reporting of any actual or suspected breach or security incident. "Security Incident" shall have the same meaning as defined under HIPAA and its implementing regulations (45 C.F.R. §164.304). User agrees to take the following steps:

A. ***Notice to DOM*****.** (1) To notify the DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer **without unreasonable delay, and no later than seventy-two (72) hours after discovery by telephone call plus email, fax, or registered or certified mail** upon the discovery of an actual or suspected breach of unsecured PHI or PI in electronic media or in any other media. (2) To notify the DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer **without unreasonable delay, and no later than seventy-two (72) hours after discovery by telephone call plus email, fax, 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 DOM by the Social Security Administration. A breach or Security Incident shall be treated as discovered by User 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 User.

The notification shall include, to the extent possible and subsequently as the information becomes available, the identification of all individuals whose unsecured PHI or PI is reasonably believed by User 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 suspect breach or Security Incident User shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the breach or Security Incident and to protect the operating environment; and
2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

B. ***Investigation and Investigation Report****.* To immediately investigate any such actual or suspected breach or Security Incident and to submit updated information by email, fax, or registered or certified mail as it becomes available to the DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer.

C. ***Complete Report.*** To provide a complete written report by email, fax, or registered or certified mail of the investigation to the DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer within ten (10) working days of the discovery of any actual or suspected breach or Security Incident. The report shall include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or Security Incident. If DOM requests information in addition to that provided in the written report, User shall make reasonable efforts to provide DOM with such information. If necessary, a supplemental report may be used to submit revised or additional information after the completed report is submitted.

D. ***Notification of Individuals.*** If the cause of an actual breach of PHI or PI is attributable to User or its subcontractors, agents or vendors, User 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 DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM 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.

E. ***Responsibility for Reporting of Breaches.*** If the cause of a breach of PHI or PI is attributable to User or its agents, subcontractors, or vendors, and User is a covered entity as defined under HIPAA and the HIPAA regulations, User 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 User has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DOM in addition to User, User shall notify DOM, and DOM and User 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.

III. ***Contact Information.*** To direct communications to the above referenced staff, User shall initiate contact as indicated herein. The parties reserve the right to make changes to the contact information below by giving written notice to User. Said changes shall not require an amendment to this Attachment or the Agreement to which it is incorporated.

DOM Point-of-Contact: See Data Use Agreement to which this Attachment is incorporated.

DOM Security Officer:	Address:	550 High Street, Suite 1000, Jackson, MS 39201
	Email:	securityofficer@medicaid.ms.gov
	Telephone:	(601) 359-6405
	Fax:	(601)-359-6294
DOM Privacy Officer:	Address:	550 High Street, Suite 1000, Jackson, MS 39201
	Email:	privacyofficer@medicaid.ms.gov
	Telephone:	(601) 359-6097
	Fax:	(601)-359-6294