

SCHEDULE F - HIPAA BUSINESS ASSOCIATE AGREEMENT

The parties to this Business Associate Agreement (“Agreement”) are the Michigan Department of Technology, Management and Budget (“DTMB”, “Business Associate 1”) on behalf of the Michigan Department of Health and Human Services (“Covered Entity”) and [Insert Name of Contractor who will be handling PHI] “Business Associate 2”.

RECITALS

- A. Under this Agreement, Business Associate 2 will collect or receive certain information on the Covered Entity’s behalf, some of which may constitute Protected Health Information (“PHI”). In consideration of the receipt of PHI, the Business Associate agrees to protect the privacy and security of the information as set forth in this Agreement.
- B. Covered Entity and each Business Associate intend to protect the privacy and provide for the security of PHI collected or received by the Business Associate under the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”) and the HIPAA Rules, as amended.
- C. The HIPAA Rules require the Covered Entity to enter into an agreement containing specific requirements with Business Associate 1, and likewise Business Associate 1 must enter an agreement with Business Associate 2 before the Business Associate 2’s receipt of PHI.

AGREEMENT

1. Definitions.

- a. The following terms used in this Agreement have the same meaning as those terms in the HIPAA Rules: Breach; Data Aggregation; Designated Record Set; Disclosure; Health Care Obligations; Individual; Minimum Necessary; Notice of Privacy Practices; Protected Health Information; Required by Law; Secretary; Security Incident; Security Measures, Subcontractor; Unsecured Protected Health Information, and Use.
- b. “Business Associate” has the same meaning as the term “business associate” at 45 CFR 160.103 and regarding this Agreement means DTMB (“Business Associate 1”) and [Insert Name of Contractor] (“Business Associate 2”).
- c. “Covered Entity” has the same meaning as the term “covered entity” at 45 CFR 160.103 and regarding this Agreement means the [Insert Name of End-User Agency whose PHI is involved].
- d. “HIPAA Rules” means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. Obligations of Business Associate 2.

Business Associate 2 agrees to:

- a. use and disclose PHI only as permitted or required by this Agreement or as required by law.

- b. implement and use appropriate safeguards and comply with Subpart C of 45 CFR 164 regarding electronic protected health information, to prevent use or disclosure of PHI other than as provided in this Agreement. Business Associate 2 must maintain, and provide a copy to the Covered Entity and Business Associate 1 within 10 days of a request from the Covered Entity or Business Associate 1, a comprehensive written information privacy and security program that includes security measures that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI relative to the size and complexity of Business Associate 2's operations and the nature and the scope of its activities.
- c. report to the Covered Entity and Business Associate 1 within 24 hours of any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of Unsecured Protected Health Information as required by 45 CFR 164.410, and any Security Incident of which it becomes aware. If Business Associate 2 is responsible for any unauthorized use or disclosure of PHI, it must promptly act as required by applicable federal and State laws and regulations. Covered Entity and Business Associate 2 will cooperate in investigating whether a breach has occurred, to decide how to provide breach notifications to individuals, the federal Health and Human Services' Office for Civil Rights, and potentially the media.
- d. ensure, according to 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate 2 agree to the same restrictions, conditions, and requirements that apply to Business Associate 2 regarding such information. Each subcontractor must sign an agreement with Business Associate 2 containing substantially the same provisions as this Agreement and further identifying Business Associate 1 and Covered Entity as a third-party beneficiary of the agreement with the subcontractor. Business Associate 2 must implement and maintain sanctions against subcontractors that violate such restrictions and conditions and must mitigate the effects of any such violation.
- e. make available PHI in a Designated Record Set to the Covered Entity within 10 days of a request from the Covered Entity to satisfy the Covered Entity's obligations under 45 CFR 164.524.
- f. within ten days of a request from the Covered Entity, amend PHI in a Designated Record Set under, 45 CFR § 164.526. If any individual requests an amendment of PHI directly from Business Associate 2 or its agents or subcontractors, Business Associate 2 must notify the Covered Entity in writing within five days of the request and amend the information within ten days of the request. Any denial of amendment of PHI maintained by Business Associate 2 or its agents or subcontractors is the responsibility of Business Associate 2.
- g. maintain, and within ten days of a request from the Covered Entity make available, the information required to provide an accounting of disclosures to enable the Covered Entity to fulfill its obligations under 45 CFR § 164.528. Business Associate 2 is not required to provide an accounting to the Covered Entity of disclosures: (i) to carry out treatment, payment or health care operations, as set forth in 45 CFR § 164.506; (ii) to individuals of PHI about them as set forth in 45 CFR § 164.502; (iii) under an authorization as provided in 45 CFR § 164.508; (iv) to persons involved in the individual's care or other notification purposes as set forth in 45 CFR § 164.510; (v) for national security or intelligence purposes as set forth in 45 CFR § 164.512(k)(2); (vi) to correctional institutions or law enforcement officials as set forth in 45 CFR § 164.512(k)(5); (vii) as part of a limited data set according to 45 CFR

164.514(e); or (viii) that occurred before the compliance date for the Covered Entity.

Business Associate 2 agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate 2 and its agents or subcontractors for at least six years before the request, but not before the compliance date of the Privacy Rule. At a minimum, such information must include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or a copy of the written request for disclosure. If the request for an accounting is delivered directly to Business Associate 2 or its agents or subcontractors, Business Associate 2 must, within ten days of the receipt of the request, forward it to the Covered Entity in writing.

- h. to the extent Business Associate 2 is to carry out one or more of the Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity when performing those obligations.
- i. make its internal practices, books, and records relating to Business Associate 2's use and disclosure of PHI available to the Secretary for purposes of determining compliance with the HIPAA Rules. Business Associate 2 must concurrently provide to the Covered Entity a copy of any PHI that the Business Associate 2 provides to the Secretary.
- j. retain all PHI throughout the term of the Agreement and for a period of six years from the date of creation or the date when it last was in effect, whichever is later, or as required by law. This obligation survives the termination of the Agreement.
- k. implement policies and procedures for the final disposition of PHI and the hardware and equipment on which it is stored, including but not limited to, removal of PHI before re-use.
- l. within ten days of a written request by the Covered Entity, Business Associate 2 and its agents or subcontractors must allow the Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of PHI under this Agreement. Business Associate 2 and the Covered Entity will mutually agree in advance upon the scope, timing and location of such an inspection. Covered Entity must protect the confidentiality of all confidential and proprietary information of Business Associate 2 to which the Covered Entity has access during the course of such inspection. Covered Entity and Business Associate 2 will execute a nondisclosure agreement, if requested by the other party. The fact that the Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate 2's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate 2 of its responsibility to comply with this Agreement. Covered Entity's (i) failure to detect or (ii) detection, but failure to notify Associate or require Associate's remediation of any unsatisfactory practices, does not constitute acceptance of such practice or a waiver of the Covered Entity's enforcement rights under this Agreement.

3. Permitted Uses and Disclosures by the Business Associate.

- a. Business Associate 2 may use or disclose PHI:
 - 1) for the proper management and administration of Business Associate 2 or to carry out the legal responsibilities of Business Associate 2; provided, however, either (A) the disclosures are required by law, or (B) Business Associate 2 obtains reasonable assurances from the person to whom the information is disclosed that the information

will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate 2 of any instances of which it is aware in which the confidentiality of the information has been breached;

- 2) as required by law;
 - 3) for Data Aggregation services relating to the health care operations of the Covered Entity;
 - 4) to de-identify, consistent with 45 CFR 164.514(a) – (c), PHI it receives from the Covered Entity. If Business Associates 2 de-identifies the PHI it receives from the Covered Entity, Business Associate 2 may use the de-identified information for any purpose not prohibited by the HIPAA Rules; and
 - 5) for any other purpose listed here: Purposes outside the scope of the Contract are not permissible.
- b. Business Associate 2 agrees to make uses and disclosures and requests for PHI consistent with the Covered Entity's minimum necessary policies and procedures.
 - c. Business Associate 2 may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by the Covered Entity except for the specific uses and disclosures described above in 3(a)(i) and (iii).

4. Covered Entity's Obligations.

Covered entity agrees to:

- a. use its Security Measures to reasonably and appropriately maintain and ensure the confidentiality, integrity, and availability of PHI transmitted to Business Associate 2 under this Agreement until the PHI is received by Business Associate 2.
- b. provide Business Associate 2 with a copy of its Notice of Privacy Practices and must notify the Business Associate of any limitations in the Notice of Privacy Practices of the Covered Entity under 45 CFR 164.520 to the extent that such limitation may affect Business Associate 2's use or disclosure of PHI.
- c. notify Business Associate 2 of any changes in, or revocation of, the permission by an individual to use or disclose the individual's PHI to the extent that such changes may affect Business Associate 2's use or disclosure of PHI.
- d. notify Business Associate 2 of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR 164.522 to the extent that such restriction may affect Business Associate 2's use or disclosure of PHI.

5. Term. This Agreement continues in effect until terminated or is replaced with a new agreement between the parties containing provisions meeting the requirements of the HIPAA Rules, whichever first occurs.

6. Termination.

- a. Material Breach. In addition to any other provisions in the Agreement regarding breach, a breach by Business Associate 2 of any provision of this Agreement, as determined by the Covered Entity, constitutes a material breach of the Agreement and provides grounds for Business Associate 1 to terminate this Agreement for cause at the request of Covered Entity. Termination for cause is subject to 6.b.

- 1) Default. If Business Associate 2 refuses or fails to timely perform any of the provisions of this Agreement, the Covered Entity may notify Business Associate 2 in writing of the non-performance, and if not corrected within thirty days, Business Associate 1 may immediately terminate the Agreement at the request of Covered Entity. The Business Associate 2 must continue performance of the Agreement to the extent it is not terminated.
 - 2) Business Associate 2's Duties. Notwithstanding termination of the Agreement, and subject to any directions from the Covered Entity or Business Associate 1, Business Associate 2 must protect and preserve property in the possession of Business Associate 2 in which the Covered Entity has an interest.
 - 3) Erroneous Termination for Default. If Business Associate 1 terminates this Agreement at the request of Covered Entity under Section 6(a) and after such termination it is determined, for any reason, that Business Associate 2 was not in default, then such termination will be treated as a termination for convenience, and the rights and obligations of the parties will be the same as if the Agreement had been terminated for convenience.
- b. Reasonable Steps to Cure Breach. If the Covered Entity or Business Associate 1 knows of a pattern of activity or practice of Business Associate 2 that constitutes a material breach or violation of Business Associate 2's obligations under the provisions of this Agreement or another arrangement and does not terminate this Agreement under Section 6(a), then the Business Associate 1, at the request of Covered Entity or on its own accord, must notify Business Associate 2 of the pattern of activity or practice. Business Associate 2 must then take reasonable steps to cure such breach or end such violation, as applicable. If the Business Associate 2's efforts to cure such breach or end such violation are unsuccessful, Business Associate 1, at the request of the Covered Entity or on its own accord, may either (i) terminate this Agreement, if feasible or (ii) report Business Associate 2's breach or violation to the Secretary.
- c. Effect of Termination. After termination of this Agreement for any reason, the Business Associate, with respect to PHI it received from the Covered Entity, or created, maintained, or received by Business Associate 2 on behalf of the Covered Entity, must:
- 1) retain only that PHI which is necessary for Business Associate 2 to continue its proper management and administration or to carry out its legal responsibilities;
 - 2) return to the Covered Entity (or, if agreed to by the Covered Entity in writing, destroy) the remaining PHI that Business Associate 2 still maintains in any form;
 - 3) continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate 2 retains the PHI;
 - 4) not use or disclose the PHI retained by Business Associate 2 other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section 3(a)(1) which applied before termination; and
 - 5) return to the Covered Entity (or, if agreed to by the Covered Entity in writing, destroy) the PHI retained by Business Associate 2 when it is no longer needed by Business Associate 2 for its proper management and administration or to carry out its legal responsibilities.

7. No Waiver of Immunity. The parties do not intend to waive any of the immunities, rights, benefits, protection, or other provisions of the Michigan Governmental Immunity Act, MCL 691.1401, et seq., the Federal Tort Claims Act, 28 U.S.C. 2671 et seq., or the common law.
8. Data Ownership. Business Associate 2 has no ownership rights in the PHI. The covered entity retains all ownership rights of the PHI.
9. Disclaimer. Neither Business Associate 1, nor the Covered Entity, warrants or represents that compliance by Business Associate 2 with this Agreement, HIPAA, or the HIPAA Rules will be adequate or satisfactory for Business Associate 2's own purposes. Business Associate 2 is solely responsible for all decisions made by Business Associate 2 regarding the safeguarding of PHI.
10. Certification. If the Covered Entity determines an examination is necessary to comply with the Covered Entity's legal obligations under HIPAA relating to certification of its security practices, the Covered Entity or its authorized agents or contractors, may, at the Covered Entity's expense, examine Business Associate 2's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to the Covered Entity the extent to which Business Associate 2's security safeguards comply with HIPAA, the HIPAA Rules or this Agreement.
11. Amendment. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA and the HIPAA Rules. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Agreement embodying written assurances consistent with the standards and requirements of HIPAA and the HIPAA Rules. Either party may terminate the Agreement upon thirty days written notice if (i) one party does not promptly enter into negotiations to amend this Agreement when requested by the other party or (ii) Business Associate 2 does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that the Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA or the HIPAA Rules.
12. Assistance in Litigation or Administrative Proceedings. Business Associate 2 must make itself, and any subcontractors, employees or agents assisting Business Associate 2 in the performance of its obligations under this Agreement, available to the Covered Entity or Business Associate 1, at no cost to the Covered Entity or Business Associate 1, to testify as witnesses, or otherwise, if litigation or administrative proceedings are commenced against the Covered Entity or Business Associate 1, its directors, officers or employees, departments, agencies, or divisions based upon a claimed violation of HIPAA or the HIPAA Rules or other laws relating to Business Associate 2's or its subcontractors use or disclosure of PHI under this Agreement, except where Business Associate 2 or its subcontractor, employee or agent is a named adverse party.
13. No Third-Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer upon any person other than the Covered Entity, Business Associate 1, Business Associate 2 and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

14. Interpretation and Order of Precedence. Any ambiguity in this Agreement must be interpreted to permit compliance with the HIPAA Rules. Where the provisions of this Agreement differ from those mandated by the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of this Agreement control.
15. Effective Date. This Agreement is effective upon receipt of the last approval necessary and the affixing of the last signature required.
16. Survival of Certain Agreement Terms. Notwithstanding any contrary provision in this Agreement, the Business Associate 2's obligations under Section 6(d) and record retention laws ("Effect of Termination") and Section 12 ("No Third-Party Beneficiaries") survive termination of this Agreement and are enforceable by the Covered Entity or Business Associate 1.
17. Representatives and Notice.
 - a. Representatives. The individuals listed below are designated as the parties' respective representatives for purposes of this Agreement. Either party may from time to time designate in writing new or substitute representatives.
 - b. Notices. All required notices must be in writing and must be hand delivered or given by certified or registered mail to the representatives at the addresses set forth below.

Covered Entity Representative:

James Bowen
Privacy and Security Manager
MDHHS Compliance Office
333 South Grand Ave, 4th Floor
Lansing, MI 48933
(517) 284-1018
MDHHSPrivacySecurity@michigan.gov

Business Associate 1 Representative:

Name: Marissa Gove
Title: Category Specialist
Department: Department of Technology, Management & Budget
Address: 320 South Walnut Street, Lansing, MI 48933
Phone: 517-449-8952
Email: Govern1@michigan.gov

Business Associate 2 Representative:

Name: [REDACTED]
Title: [REDACTED]
Department: [REDACTED]
Address: [REDACTED]
Phone: [REDACTED]
Email: [REDACTED]

Any notice given to a party under this Agreement shall be deemed effective, if addressed to such party, upon: (i) delivery, if hand delivered; or (ii) the third Business Day after being sent by certified or registered mail.

**DTMB as Business Associate 1 on
behalf of the Michigan Department
of Health and Human Services**

Business Associate 2

By: _____

By: _____

Date: _____

Date: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____