

## HIPAA BUSINESS ASSOCIATE AGREEMENT

This HIPAA Business Associate Agreement (“Agreement”) is made by and between \_\_\_\_\_ (“Covered Entity”) and Healthcare Blocks, Inc. (“Associate”).

Covered Entity and Associate agree that the parties are entering this Agreement in order to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act (“HITECH”) and their implementing regulations set forth at 45 C.F.R. Parts 160 and Part 164 (the “HIPAA Rules”). To the extent Associate is acting as a Business Associate of Covered Entity pursuant to the Agreement, the provisions of this Agreement shall apply, and Associate shall be subject to the penalty provisions of HIPAA as specified in 45 CFR Part 160.

The parties have entered in to an underlying agreement (the “Agreement”) pursuant to which Healthcare Blocks provides certain services for or on behalf of Client, which may require access to, or the use disclosure of PHI that is subject to protection under HIPAA.

**1. Definitions.** Capitalized terms not otherwise defined in this Agreement shall have the meaning set forth in the HIPAA Rules. References to “PHI” mean Protected Health Information maintained, created, received or transmitted by Associate from Covered Entity or on Covered Entity’s behalf.

**2. Uses or Disclosures.** Associate will neither use nor disclose PHI except as permitted or required by this Agreement or as required by law. To the extent Associate is to carry out an obligation of Covered Entity under the HIPAA Rules, Associate shall comply with the requirements of the HIPAA Rules that apply to Covered Entity in the performance of such obligation. Without limiting the foregoing, Associate will not sell PHI or use or disclose PHI for purposes of marketing or fundraising, as defined and proscribed in the HIPAA Rules and HITECH. Associate is permitted to use and disclose PHI:

(a) to perform any and all obligations of Associate as described in the Agreement, provided that such use or disclosure would not violate the HIPAA Rules, if done by Covered Entity directly;

(b) as otherwise permitted by law, provided that such use or disclosure would not violate the HIPAA Rules, if done by Covered Entity directly and provided that Covered Entity gives its prior written consent;

(c) to perform Data Aggregation services relating to Covered Entity’s health care operations;

(d) to report violations of the law to federal or state authorities consistent with 45 CFR § 164.502(j)(1);

(e) as necessary for Associate’s proper management and administration and to carry out Associate’s legal responsibilities (collectively “Associate’s Operations”), provided that Associate may only disclose PHI for Associate’s Operations if the disclosure is Required By

Law or Associate obtains reasonable assurance, evidenced by a written contract, from the recipient that the recipient will: (1) hold such PHI in confidence and use or further disclose it only for the purpose for which it was disclosed or as Required By Law; and (2) notify Associate of any instance of which the recipient becomes aware in which the confidentiality of such PHI was breached;

(f) to de-identify PHI in accordance with 45 CFR § 164.514(b), provided that such de-identified information may be used and disclosed only consistent with applicable law.

In the event Covered Entity notifies Associate of a restriction request that would restrict a use or disclosure otherwise permitted by this Agreement, Associate shall comply with the terms of the restriction request.

**3. Safeguards.** Associate will use appropriate administrative, technical and physical safeguards to prevent the use or disclosure of PHI other than as permitted by this Agreement. Associate will also comply with the provisions of 45 CFR Part 164, Subpart C of the HIPAA Rules with respect to electronic PHI to prevent any use or disclosure of such information other than as provided by this Agreement.

**4. Subcontractors and Agents.** In accordance with 45 CFR §§ 164.308(b)(2) and 164.502(e)(1)(ii), Associate will ensure that all of its subcontractors and agents that create, receive, maintain or transmit PHI on behalf of Associate agree by written contract to comply with the same restrictions and conditions that apply to Associate with respect to such PHI.

**5. Minimum Necessary.** Associate represents that the PHI requested, used or disclosed by Associate shall be the minimum amount necessary to carry out the purposes of the Agreement. Associate will limit its uses and disclosures of, and requests for, PHI (i) when practical, to the information making up a Limited Data Set; and (ii) in all other cases subject to the requirements of 45 CFR § 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

**6. Covered Entity Obligations.** Covered Entity shall notify Associate of (i) any limitations in its notice of privacy practices, (ii) any changes in, or revocation of, permission by an individual to use or disclose PHI, and (iii) any confidential communication request or restriction on the use or disclosure of PHI affecting Associate that Covered Entity has agreed to or with which Covered Entity is required to comply, to the extent any of the foregoing affect Associate's use or disclosure of PHI.

**7. Access and Amendment.** In accordance with 45 CFR § 164.524, Associate shall permit Covered Entity or, at Covered Entity's request, an Individual (or the Individual's personal representative) to inspect and obtain copies of any PHI about the Individual that is in Associate's custody or control and that is maintained in a Designated Record Set. If the requested PHI is maintained electronically, Associate must provide a copy of the PHI in the electronic form and format requested by the Individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual. Associate will, upon receipt of notice from Covered Entity, promptly amend or permit Covered Entity access to amend PHI so that Covered Entity may meet its amendment obligations under 45 CFR § 164.526.

**8. Accounting.** Except for disclosures excluded from the accounting obligation by the HIPAA Rules and regulations issued pursuant to HITECH, Associate will record for each disclosure that Associate makes of PHI the information necessary for Covered Entity to make an accounting of disclosures pursuant to the HIPAA Rules. In the event the U.S. Department of Health and Human Services (“HHS”) finalizes regulations requiring Covered Entities to provide access reports, Associate shall also record such information with respect to electronic PHI held by Associate as would be required under the regulations for Covered Entities beginning on the effective date of such regulations. Associate will make information required to be recorded pursuant to this Section available to Covered Entity promptly upon Covered Entity’s request for the period requested, but for no longer than required by the HIPAA Rules (except Associate need not have any information for disclosures occurring before the effective date of this Agreement)..

**9. Inspection of Books and Records.** Associate will make its internal practices, books, and records, relating to its use and disclosure of PHI, available upon request to HHS to determine compliance with the HIPAA Rules.

**10. Reporting.** To the extent Associate becomes aware or discovers any use or disclosure of PHI not permitted by this Agreement, any Security Incident involving electronic PHI or any Breach of Unsecured Protected Health Information, Associate shall promptly report such use, disclosure, Security Incident or Breach to Covered Entity. Associate shall mitigate, to the extent practicable, any harmful effect known to it of a Breach or negligent use or disclosure of PHI by Associate not permitted by this Agreement. With respect to Breaches, the report shall include to the extent known (1) the identification of each Individual whose PHI has been, or is reasonably believed by Associate to have been, accessed, acquired, or disclosed during the Breach; (2) a description of the types of PHI that may have been involved in the Breach; and (3) a brief description of the circumstances surrounding the Breach, including the date of the Breach and the date that the Breach was discovered. Notwithstanding the foregoing, the parties acknowledge and agree that this section constitutes notice by Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. “Unsuccessful Security Incidents” shall include, but not be limited to, pings and other broadcast attacks on Associate’s firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of electronic PHI. All reports of Breaches shall be made in compliance with 45 CFR § 164.410. In the event that a law enforcement official instructs Associate to delay notification of a Breach to Covered Entity, Associate shall be permitted to do so; provided, however, that if a law enforcement official’s instructions are oral, Associate may not delay notification to Covered Entity more than thirty (30) days from the date of the oral statement unless, during such thirty (30) day period, Associate receives a written statement from a law enforcement official that specifies a longer time period to delay notification.

**11. Term.** This Agreement shall be effective as of the effective date of the Agreement and shall remain in effect until termination of the Agreement. Either party may terminate this Agreement and the Agreement effective immediately if it determines that the other party has breached a material provision of this Agreement and failed to cure such breach within thirty (30) days of being notified by the other party of the breach. If the non-breaching party determines that cure is not possible, such party may terminate this Agreement and the Agreement effective

immediately upon written notice to other party. If termination is not feasible, the non-breaching party shall report the breach to HHS.

Upon termination of this Agreement for any reason, Associate will, if feasible, return to Covered Entity or securely destroy all PHI maintained by Associate in any form or medium, including all copies of such PHI. Further, Associate shall recover any PHI in the possession of its agents and subcontractors and return to Covered Entity or securely destroy all such PHI. In the event that Associate determines that returning or destroying any PHI is infeasible, Associate may maintain such PHI but shall continue to abide by the terms and conditions of this Agreement with respect to such PHI and shall limit its further use or disclosure of such PHI to those purposes that make return or destruction of the PHI infeasible. Upon termination of this Agreement for any reason, all of Associate's obligations under this Agreement shall survive termination and remain in effect (a) until Associate has completed the return or destruction of PHI as required by Section and (b) to the extent Associate retains any PHI pursuant to this Section.

**12. General Provisions.** In the event that any final regulation or amendment to final regulations is promulgated by HHS or other government regulatory authority with respect to PHI, the parties shall negotiate in good faith to amend this Agreement to remain in compliance with such regulations. Any ambiguity in this Agreement shall be resolved to permit Covered Entity and Associate to comply with the HIPAA Rules. Nothing in this Agreement shall be construed to create any rights or remedies in any third parties or any agency relationship between the parties. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended. The terms and conditions of this Agreement override and control any conflicting term or condition of the Agreement and replace and supersede any prior business associate agreements in place between the parties. All non-conflicting terms and conditions of the Agreement remain in full force and effect.

[remainder of page intentionally left blank]

**IN WITNESS WHEREOF**, the parties hereto have executed this Agreement by their duly-authorized representatives.

Entity:	Entity: <b>Healthcare Blocks</b>
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date: