



## **HIPAA BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement, dated as of September 22, 2014 (“BA Agreement”), supplements and is made a part of the Services Agreement (as defined below) by and between \_\_\_\_\_ (“Covered Entity”) and **Healthix, Inc.** (“Business Associate”). Covered Entity and Business Associate may be referred to herein collectively as the “Parties” or individually as “Party”.

WHEREAS, Covered Entity and Business Associate are parties to the Services Agreement pursuant to which Business Associate provides certain services to Covered Entity. In connection with Business Associate’s services, Business Associate creates, receives, maintains or transmits Protected Health Information from or on behalf of Covered Entity, which information is subject to protection under the Federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”), and related regulations promulgated by the Secretary (“HIPAA Regulations”); and

WHEREAS, Business Associate qualifies as a “business associate” (as defined by the HIPAA Regulations) of its clients, which means that Business Associate has certain responsibilities with respect to the Protected Health Information of its clients; and

WHEREAS, in light of the foregoing and the requirements of HIPAA, the HITECH Act, and HIPAA Regulations, Business Associate and Covered Entity agree to be bound by the following terms and conditions.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree in this BA Agreement as follows:

### **1. Definitions.**

(a) General. Terms used, but not otherwise defined, in this BA Agreement shall have the same meaning given to those terms by HIPAA, the HITECH Act and HIPAA Regulations as in effect or as amended from time to time.

(b) Specific.

(i) Breach. “Breach” shall have the same meaning as the term “breach” in 45 CFR § 164.402.

(ii) Data Aggregation Services. “Data Aggregation Services” shall mean the combining of Protected Health Information by Business Associate with the Protected Health Information received by Business Associate in its capacity as a business associate of a HIPAA covered entity, to permit data analyses that relate to health care operations of the respective covered entities.

(iii) Electronic Health Record. “Electronic Health Record” shall have the same meaning as the term “electronic health record” in the HITECH Act, Section 13400(5).

(iv) Electronic Protected Health Information. “Electronic Protected Health Information” shall have the same meaning as the term “electronic protected health information” in 45 CFR § 160.103, limited to the information that Business Associate creates, receives, maintains, or transmits from or on behalf of Covered Entity.

(v) Individual. “Individual” shall have the same meaning as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

(vi) Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164.

(vii) Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103, limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

(viii) Required By Law. “Required by Law” shall have the same meaning as the term “required by law” in 45 CFR § 164.103.

(ix) Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

(x) Security Rule. “Security Rule” shall mean the Security Standards at 45 Part 160 and Part 164.

(xi) Services Agreement. “Services Agreement” shall mean any present or future agreements, either written or oral, between Covered Entity and Business Associate under which Business Associate provides services to Covered Entity which involve the use or disclosure of Protected Health Information. The Services Agreement is amended by and incorporates the terms of this BA Agreement.

(xii) Statewide Policy Guidance. “Statewide Policy Guidance” shall mean the set of policies and procedures, including technical standards, adopted by the New York State Department of Health, related to operation of the Statewide Health Information Network of New York, or SHIN-NY.

(xiii) Subcontractor. “Subcontractor” shall have the same meaning as the term “subcontractor” in 45 CFR § 160.103.

(xiv) Unsecured Protected Health Information. “Unsecured Protected Health Information” shall have the same meaning as the term “unsecured protected health information” in 45 CFR § 164.402.

## **2. Obligations and Activities of Business Associate.**

(a) Use and Disclosure. Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by the Services Agreement, this BA Agreement, Statewide Policy Guidance or as Required By Law. Business Associate shall comply with the provisions of this BA Agreement relating to privacy and security of Protected Health Information and all present and future provisions of HIPAA, the HITECH Act and HIPAA Regulations that relate to the privacy and security of Protected Health Information and that are applicable to Covered Entity and/or Business Associate. Without limiting the foregoing, to the extent the Business Associate will carry out one or more of the Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

(b) Appropriate Safeguards. Business Associate agrees to use appropriate safeguards and comply, where applicable, with the Security Rule (with respect to Electronic Protected Health Information) to prevent the use or disclosure of the Protected Health Information other than as provided for by this BA Agreement. Without limiting the generality of the foregoing sentence, Business Associate will:

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information as required by the Security Rule; and

(ii) Ensure that any Subcontractor to whom Business Associate provides Electronic Protected Health Information agrees in writing to implement reasonable and appropriate safeguards and comply, where applicable, with the Security Rule to protect Electronic Protected Health Information and comply with the other requirements of Section 2(a) above.

(c) Reporting. Business Associate agrees to promptly, and at most within three (3) business days, report to Covered Entity any of the following:

(i) Any use or disclosure of Protected Health Information not permitted by this BA Agreement of which Business Associate becomes aware.

(ii) Any Security Incident of which Business Associate becomes aware.

(iii) The discovery of a Breach of Unsecured Protected Health Information. A Breach is considered "discovered" as of the first day on which the Breach is known, or reasonably should have been known, to Business Associate or any employee, officer or agent of Business Associate, other than the individual committing the Breach. Any notice of a Security Incident or Breach of Unsecured Protected Health Information shall include the identification of each Individual whose Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired or disclosed during such Security Incident or Breach as well as any other relevant information regarding the Security Incident or Breach. Any such notice shall be directed to Covered Entity as set forth in the Services Agreement.

(d) 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 Protected Health Information by Business Associate or its employees, officers, Subcontractors or agents in

violation of the requirements of this BA Agreement (including, without limitation, any Security Incident or Breach of Unsecured Protected Health Information).

(e) Subcontractors. Business Associate shall ensure that any Subcontractor to whom Business Associate provides Protected Health Information received from, or created, maintained, received or transmitted by, Business Associate on behalf of Covered Entity agrees in writing to the same restrictions and conditions that apply through this BA Agreement to Business Associate with respect to such information.

(f) Access to Designated Record Sets. To the extent that Business Associate possesses or maintains Protected Health Information in a Designated Record Set, Business Associate agrees to provide access, at the request of Covered Entity to Protected Health Information in a Designated Record Set, to Covered Entity in order to meet the requirements under HIPAA Regulations. If an Individual makes a request for access to Protected Health Information directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

(g) Amendments to Designated Record Sets. To the extent that Business Associate possesses or maintains Protected Health Information in a Designated Record Set, Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to HIPAA Regulations at the request of Covered Entity or an Individual. If an Individual makes a request for an amendment to Protected Health Information directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

(h) Access to Books and Records. Business Associate agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

(i) Accountings. Business Associate agrees to document such disclosures of Protected Health Information 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 Protected Health Information in accordance with HIPAA, HIPAA Regulations and the HITECH Act.

(j) Requests for Accountings. Business Associate agrees to provide to Covered Entity, within twenty (20) days of a request by Covered Entity, information collected in accordance with Section 2(i) of this BA Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with HIPAA, HIPAA Regulations and the HITECH Act. If an Individual makes a request for an accounting directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

### **3. Permitted Uses and Disclosures by Business Associate.**

(a) Services Agreement. Except as otherwise limited in this BA Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Services Agreement, provided that such use or disclosure would not violate HIPAA, HIPAA Regulations or the HITECH Act if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

(i) Data Aggregation Services. Except as otherwise limited in this BA Agreement, Business Associate may provide Data Aggregation Services as permitted by 45 CFR § 164.504(e)(2)(i)(B) and may use and disclose data sets resulting from Data Aggregation Services as permitted by the Services Agreement.

(ii) De-Identified Data. Except as otherwise limited in this BA Agreement, Business Associate may de-identify Protected Health Information received from Covered Entity in accordance with 45 CFR § 164.514 and may use and disclose such de-identified Protected Health Information as permitted by the Services Agreement.

(iii) Limited Data Sets. Except as otherwise limited in this BA Agreement, Business Associate may create Limited Data Sets using Protected Health Information received from Covered Entity in accordance with 45 CFR § 164.514 and may use and disclose such Limited Data Sets as permitted by the Services Agreement.

(b) Use for Administration of Business Associate. Except as otherwise limited in this BA Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(c) Disclosure for Administration of Business Associate. Except as otherwise limited in this BA Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that (i) disclosures are Required by Law, or (ii) 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.

**4. Permissible Requests by Covered Entity.** Except as set forth in Section 3 of this BA Agreement, Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

### **5. Term and Termination.**

(a) Term. This BA Agreement shall be effective as of the date of this BA Agreement and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created, received or maintained by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or

destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination for Cause. Upon either Party's knowledge of a material breach by the other Party of the terms of this BA Agreement, the non-breaching Party shall either:

(i) Provide an opportunity for the other Party to cure the breach or end the violation. If such Party does not cure the breach or end the violation within thirty (30) days, the non-breaching Party shall terminate: (A) this BA Agreement; (B) all of the provisions of the Services Agreement that involve the use or disclosure of Protected Health Information; and (C) such other provisions, if any, of the Services Agreement as the non-breaching Party designates in its sole discretion; or

(ii) Notwithstanding anything contained in the Services Agreement to the contrary, if the other Party has breached a material term of this BA Agreement and cure is not possible, immediately terminate: (A) this BA Agreement; (B) all of the provisions of the Services Agreement that involve the use or disclosure of Protected Health Information; and (C) such other provisions, if any, of the Services Agreement as the non-breaching Party designates in its sole discretion.

(c) Effect of Termination.

(i) Except as provided in Section 5(c)(ii), upon termination of this BA Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(ii) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Business Associate shall extend the protections of this BA Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

## **6. Obligations of Covered Entity.**

(a) Privacy Notice. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b) Changes of Permission of Individual. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Restrictions on Use or Disclosure. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

## **7. Coordination of Business Associate and Covered Entity.**

(a) Investigation. The Parties shall reasonably cooperate and coordinate with each other in the investigation of any violation of the requirements of this BA Agreement and/or any Security Incident or Breach.

(b) Reports and Notices. The Parties shall reasonably cooperate and coordinate with each other in the preparation of any reports or notices to the Individual, a regulatory body or any third party required to be made under HIPAA, HIPAA Regulations, the HITECH Act, or any other Federal or State laws, rules or regulations.

## **8. Miscellaneous.**

(a) No HIPAA Agency Relationship. It is not intended that an agency relationship (as defined under the Federal common law of agency) be established hereby expressly or by implication between Covered Entity and Business Associate for purposes of liability under HIPAA, HIPAA Regulations, or the HITECH Act. No terms or conditions contained in this BA Agreement shall be construed to make or render Business Associate an agent of Covered Entity.

(b) Regulatory References. A reference in this BA Agreement to a section in HIPAA, HIPAA Regulations, or the HITECH Act means the section as in effect or as amended or modified from time to time, including any corresponding provisions of subsequent superseding laws or regulations.

(c) Amendment. The Parties agree to take such action as is necessary to amend the Services Agreement and/or this BA Agreement from time to time as is necessary for Covered Entity to comply with the requirements of HIPAA, the HIPAA Regulations and the HITECH Act.

(d) Survival. The rights and obligations of Business Associate under Sections 5(c) and the Parties under Section 7 and this Section 8 of this BA Agreement shall survive the termination of the Services Agreement and this BA Agreement.

(e) Interpretation. Any ambiguity in this BA Agreement shall be resolved to permit both Parties to comply with HIPAA, HIPAA Regulations and the HITECH Act.

(f) Miscellaneous. The terms of this BA Agreement are hereby incorporated into the Services Agreement. Except as otherwise set forth in Section 8(d) of this BA Agreement, in the event of a conflict between the terms of this BA Agreement and the terms of the Services Agreement, the terms of this BA Agreement shall prevail. The terms of the Services Agreement which are not modified by this BA Agreement shall remain in full force and effect in accordance with the terms thereof. This BA Agreement shall be governed by, and construed in accordance with, the state where the Business Associate is located, exclusive of conflict of law rules. Each Party hereby agrees and consents that any legal action or proceeding with respect to this BA Agreement shall only be brought in the courts of the state where the Business Associate is

located in the county where the Business Associate is located. The Services Agreement together with this BA Agreement constitutes the entire agreement between the Parties with respect to the subject matter contained herein, and this BA Agreement supersedes and replaces any former business associate agreement or addendum entered into by the Parties. This BA Agreement may be executed in counterparts, each of which when taken together shall constitute one original. Any PDF or facsimile signatures to this BA Agreement shall be deemed original signatures to this BA Agreement. No amendments or modifications to the BA Agreement shall be effective unless agreed upon by both Parties in writing.

**IN WITNESS WHEREOF**, the Parties have executed this BA Agreement as of the date set forth above.

\_\_\_\_\_ **Healthix, Inc.**

By: \_\_\_\_\_  
Name:  
Title:

By: \_\_\_\_\_  
Thomas Check  
President and CEO