

## **ATTACHMENT C / HEALTH PLANS BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (“Agreement”) is entered into between West Virginia Health Information Network (the “Business Associate”) and Participating Organization (“PO”) and is effective as set forth in Section 6(a) below.

### RECITALS

A. Business Associate provides services to PO in accordance with a Participation Agreement (“Participation Agreement”).

B. Under the Participation Agreement, PO may disclose information to Business Associate which constitutes Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996, as amended by the relevant portions of the Health Information Technology for Economic and Clinical Health (“HITECH”) Act (collectively, “HIPAA”).

C. The purpose of this Agreement is to satisfy the requirements of HIPAA that Business Associate provide satisfactory written assurances to PO that it will comply with the applicable requirements of HIPAA.

In consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

1. **Definitions.** Unless otherwise defined in this Agreement, including the definitions stated in the Recitals, which are incorporated into this Section 1 by reference, capitalized terms have the meaning ascribed to them under HIPAA or in the Participation Agreement for purposes of this Business Associate Agreement.

a. **Breach.** “Breach” means the acquisition, access, use, or disclosure of a Patient’s Unsecured Protected Health Information by an unauthorized person or entity in a manner not permitted under the HIPAA privacy rules, and in a manner that otherwise satisfies all other requirements imposed by the rules governing Breach notification for Unsecured Protected Health Information in 45 C.F.R. Part 164, as may be amended.

b. **Guidance.** “Guidance” shall mean official guidance of the Secretary as specified in the HITECH Act and any other official guidance or interpretation of HIPAA by a federal governmental agency with jurisdiction.

c. **Designated Record Set.** “Designated Record Set” means any grouping of medical or billing records maintained by a Covered Entity and used to make Treatment or Payment decisions about a Patient. A Designated Record Set shall have the same meaning as such term is defined in 45 C.F.R. Part 164, Subpart E, as may be amended.

d. HIPAA. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as may be amended, and its implementing rules promulgated in 45 C.F.R. Parts 160, 162, and 164, as may be amended.

e. HIPAA Privacy Rules. "HIPAA Privacy Rules" means those privacy rules described in 45 C.F.R. Part 164, Subpart E, as modified and enlarged by the Health Information Technology for Economic and Clinical Health (HITECH) Act and any other subsequent amendments to the Rules.

f. Protected Health Information or PHI and ePHI. "Protected Health Information" and "PHI" means any information that relates to the past, present, or future physical or mental health or condition of a Patient, the provision of health care items or services to the Patient, and the past, present, or future Payment for the provision of health care items or services to a Patient. Protected Health Information also must personally identify a Patient or provide a reasonable basis to believe that the information can be used to identify a Patient. The term "Protected Health Information" shall include electronic Protected Health Information and each shall have the meaning as defined in 45 C.F.R. Part 160, as may be amended.

g. Security Incident. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

h. Security Standards. "Security Standards" shall mean the Security Standards at 45 CFR parts 160, 162 and 164, as amended by the HITECH Act and HIPAA Regulations and Guidance.

i. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

j. Subcontractor. "Subcontractor" shall mean a person or entity to which Business Associate delegates a function, activity or service involving access to PHI or ePHI of PO, other than as a member of Business Associate Workforce.

k. Unsecured. "Unsecured" as applied to Protected Health Information means Protected Health Information in any form, electronic, paper or oral, that is not secured through the use of a technology or methodology specified by the Secretary in Regulations or Guidance.

## **2. Obligations and Activities of Business Associate as to Protected Health Information.**

a. Business Associate agrees to not Use or further Disclose Protected Health Information other than as permitted or required by the Participation Agreement, this Agreement, or as Required by Law and to otherwise comply with the provisions of the Privacy Rule and the Security Rule applicable to Business Associate. This includes the restrictions on the Sale of PHI and or its Use for Marketing provided in the HIPAA

Regulations. The restrictions on the secondary use of Protected Health Information contained in the Terms and Conditions of the Participation Agreement are also specifically incorporated into this Agreement.

b. Business Associate agrees to use appropriate safeguards to prevent Use or Disclosure of Protected Health Information other than as provided for in Section 2(a.) above. If and to the extent Protected Health Information disclosed to, accessed, used, maintained, held, or created by Business Associate is ePHI, Business Associate will comply with the applicable provisions of the Security Standards, by providing Administrative, Physical, and Technical Safeguards for all ePHI and by developing Policies and Procedures implementing those Safeguards.

c. Business Associate agrees to promptly report to PO any Use or Disclosure of the Protected Health Information not provided for in the Participation Agreement and/or this Agreement. Business Associate agrees to report to PO any Breach within two (2) business days of the first day the Breach is known, or reasonably should have been known, to the Business Associate, including for this purpose known to any employee, officer, or other agent of the Business Associate (other than the individual committing the Breach) ("Breach Notice"). The Breach Notice will include the date of the Breach and the date of discovery of the Breach and, to the extent known to Business Associate at the time in the exercise of reasonable diligence, identification of each Individual whose Unsecured PHI was, or is reasonably believed by the Business Associate to have been, subject to the Breach, and the nature of the PHI that was subject to the Breach and other information required for notification of Individuals of the Breach (collectively, "Breach Information"). Business Associate will notify PO in writing of any additional Breach Information not included in the Breach Notice or of the circumstances that prevent Business Associate from obtaining such information not later than ten (10) days after the Breach Notice was sent by Business Associate. Business Associate will cooperate with PO in the further investigation of the Breach, as reasonably required or as requested by PO. The steps required of Business Associate under this Section 2(c) shall be at Business Associate's expense. If Business Associate believes that the facts related to a Breach justify the application of any statutory exceptions specified at Section 13400 of the HITECH Act and to the regulatory exclusions specified at 45 C.F.R. §164.402, Business Associate shall describe those facts in the Breach Notice and the parties shall thereafter discuss the possible application of an exception or an exclusion, provided that any final decision on the availability of an exclusion or exception will be that of the PO. The parties agree that this Section 2(d) satisfies any notices necessary by Business Associate to PO of the ongoing existence and occurrence of Unsuccessful Security Incidents for which no additional notice to PO shall be required, except on request as stated below. For purposes of this Agreement, such Unsuccessful Security Incidents include, without limitation, activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denial of service and any combination of the above, so long as no such Unsuccessful Security Incident results in unauthorized access, use, disclosure, modification or destruction of ePHI or interference with information system operations related to the ePHI, provided that, upon written request from PO, Business Associate will provide a log or similar documentation of Unsuccessful Security Incidents

for the period of time reasonably specified in PO's request. Successful Security Incidents will be reported to PO within two (2) business days of the date the Successful Security Incident is, or in the exercise of reasonable efforts should have been known, to Business Associate. If the Successful Security Incident constitutes a Breach, the parties will proceed as required under this Agreement as to a Breach.

d. Business Associate agrees to use reasonable efforts to mitigate, at its expense, any harmful effect that is known to Business Associate to result from a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of the Participation Agreement and/or this Agreement, including without limitation a Breach. Business Associate will coordinate any mitigation efforts with PO.

e. Business Associate agrees to ensure that any Subcontractor agrees, in a form meeting the requirements of 45 C.F.R. § 164.314, to substantially the same restrictions and obligations that apply through this Agreement to Business Associate with respect to Protected Health Information, including those obligations relating to ePHI. Upon Business Associate's knowledge of a pattern of activity or practice of a Subcontractor in violation of the requirements of the foregoing agreement, Business Associate will provide notice and an opportunity, not longer than a reasonable time consistent with the nature of the breach and the terms of the Service Agreement with the Subcontractor, for the Subcontractor to end the violation. Business Associate will terminate the agreement with that Subcontractor if the Subcontractor does not end the violation within the time specified by the Business Associate.

f. To the extent Business Associate maintains a Designated Record Set for the PO, Business Associate will make available, within a reasonable amount of time of receipt of a written request, Protected Health Information in the Designated Record Set in accordance with the requirements of HIPAA, including information, if any, maintained in an Electronic Designated Record Set. Business Associate will report any request for Access that it receives directly from an Individual to PO within ten (10) business days of receipt. PO will determine any appropriate limitations on such Access and the parties will determine a reasonable method for providing such Access, including, if appropriate, Transmission to a Third Party.

g. To the extent Business Associate maintains a Designated Record Set for the PO, Business Associate agrees to make an amendment, within a reasonable amount of time of receipt of a written request, to Protected Health Information in the Designated Record Set in accordance with the requirements of HIPAA. Business Associate will report any request for an amendment that it receives directly from an Individual to PO within ten (10) business days of receipt. The PO will determine and provide to Business Associate the appropriate substance of any such amendment.

h. Business Associate agrees to maintain and make available on written request information required to provide an Accounting of its Disclosures of Protected Health Information required for the PO to respond to a request by an Individual in accordance with the requirements of HIPAA. At such time as final Regulations or

Guidance as to Accounting for Disclosures for purposes of Treatment, Payment and Health Care Operations (“TPO Accounting”) are published, Business Associate will provide an amendment to this Agreement under Section 7(e) to specify the extent and manner in which TPO Accounting Information will be recorded and provided, to be effective as of the date upon which compliance with TPO Accounting Regulations or Guidance is required by PO.

i. Subject to receiving notice as described in Section 4(b), Business Associate agrees to abide by any restriction on the Use or Disclosure of PHI agreed to by PO, provided that, in the event of an agreement of PO required by HIPAA not to disclose an item or service paid for, entirely out-of-pocket, by an Individual to a Health Plan for Payment or Health Care Operations purposes, unless such Disclosure is Required by Law, the parties agree that such information shall be treated by PO as Sensitive Health Information under the Participation Agreement and will not made available to Business Associate.

j. Upon request, Business Associate will make its internal practices, books, and records relating to the Use and Disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, PO available to the Secretary for purposes of determining PO’s and Business Associate’s compliance with the HIPAA.

k. To the extent that Business Associate will carry out an obligation of PO under the Security and Privacy provisions set out in Subpart E of 45 CFR Part 164, Business Associate will perform such obligations in compliance with the provisions of such Subpart that apply to the PO as to such obligations.

3. **Permitted Uses and Disclosures of Protected Health Information by Business Associate.** Business Associate may Use or Disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, PO as specified in the Participation Agreement, provided that such Use or Disclosure would not violate the Privacy Rule if done by the PO. In addition:

a. Except as otherwise limited in this Agreement, Business Associate may Use or Disclose Protected Health Information for the proper management and administration of the Business Associate or to carry out legal responsibilities of Business Associate, provided that in the event of Disclosures, the Disclosure is Required by Law or Business Associate obtains reasonable assurances, in a form substantially similar to a Business Associate Agreement, 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 that the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

b. Business Associate may Use Protected Health Information to provide Data Aggregation services to PO to the extent provided for in the Participation Agreement.

c. Business Associate agrees that it will not De-identify any PHI to which it has access under the Participation Agreement except as for a purpose permitted under the Participation Agreement, such as Permitted Purposes and subject to any approvals required for such use under the Participation Agreement or permitted under this Agreement. Without limiting the generality of the foregoing, and regardless of what may be permitted under Applicable Law, Business Associate will not manipulate, aggregate, integrate, compile, merge, reorganize, regenerate such PHI, even if De-identified, or derive from such PHI, even if De-identified, any list, compilation, abstraction, or other information to use for a business purpose of Business Associate that is unrelated to the services Business Associate provides under the Participation Agreement (“Secondary Use”) or allow access to the PHI or any derivation of it to a third party (even if related to Business Associate) for a Secondary Use.

#### **4. Obligations of PO to Inform Business Associate of Privacy Practices and Individual Restrictions.**

a. PO shall provide Business Associate with the Notice of Privacy Practices that PO produces in accordance with HIPAA upon request by Business Associate. PO shall provide Business Associate any changes to such Notice of Privacy Practices that will affect Business Associate’s Use or Disclosure of PHI.

b. PO shall notify Business Associate of any restriction on the Use or Disclosure of Protected Health Information that PO has agreed to in accordance with the Privacy Rule, to the extent that such restriction will affect Business Associate’s Use or Disclosure of Protected Health Information. In order to allow Business Associate to comply with such agreed restriction, such notice will be provided at least fifteen (15) business days in advance of the date upon which compliance by the Business Associate is required under HIPAA.

5. **Permissible Requests or Disclosures; Minimum Necessary.** Except as specifically provided in the Participation Agreement or this Agreement, PO 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 PO, except as provided in this Agreement for Business Associate’s Data Aggregation, internal management and administration or legal responsibilities. Without limiting the generality of the foregoing, PO will provide, and Business Associate will request, no more than, the Minimum Necessary amount of PHI required for the performance of Business Associate’s services under the Participation Agreement; provided, that the Minimum Necessary requirement shall not apply to any Disclosure for Treatment or Emergency Treatment. As of the date upon which compliance is required with Guidance regarding Minimum Necessary Uses and Disclosures, Business Associate and PO will comply with such Guidance. To the extent that an amendment to this Agreement is required for such compliance, Business Associate will provide such an amendment in accordance with Section 7(e).

6. **Term and Termination**

a. **Term.** This Agreement is effective as of the Effective Date of Participation Agreement and replaces any prior Business Associate Agreement between the parties relating to this Participation Agreement. This Agreement shall terminate when the Participation Agreement terminates and all of the Protected Health Information provided by PO to Business Associate, or created or received by Business Associate on behalf of PO, is destroyed or returned to PO, or if it is not feasible to return or destroy Protected Health Information, when protections are extended to such information, in accordance with the provisions of Section 6(c.).

b. **Termination.**

i. Upon one party's knowledge of a material breach by the other party of this Agreement, the parties may proceed under the termination for cause for material breach provisions of the Participation Agreement. Notwithstanding the foregoing, if there is no termination for cause for material breach provision in the Participation Agreement, then the non-breaching party shall provide the breaching party with written notice of the material breach which describes the breach in reasonable detail and the breaching party shall have thirty (30) days from receipt of the notice to cure the breach to the reasonable satisfaction of the non-breaching party. If the breaching party has not done so within that period, the non-breaching party may terminate this Agreement for cause effective on further written notice to the breaching party;

ii. Notwithstanding the foregoing, the non-breaching party may immediately terminate this Agreement if the breaching party has breached a material term of this Agreement and the non-breaching party reasonably determines that cure is not feasible.

c. **Effect of Termination.**

i. Upon termination of this Agreement for any reason, Business Associate agrees to return or destroy (in a manner that renders the information Secure) all PHI received from, or accessed, maintained, used, disclosed and/or transmitted for or on behalf of, PO by Business Associate. If, or to the extent that, Business Associate reasonably determines that the return or destruction of PHI is not feasible, Business Associate shall inform PO in writing of the reason thereof, and agrees to extend the protections of this Agreement to such PHI and limit further Uses and Disclosures of the PHI to those purposes that make the return or destruction of the PHI not feasible until Business Associate returns or destroys the PHI.

ii. Notwithstanding the foregoing, PO and Business Associate agree that, as provided in the Participation Agreement, Protected Health Information that has been provided to other Participants in accordance with the Participation Agreement is not subject to the foregoing requirements. In addition, Protected Health Information of Participant that is incorporated into Business Associate's Health Information Exchange Master Patient Index and Registry, in accordance with and as defined in the Participation

Agreement, may be retained by Business Associate for purpose of indexing and record location for records that were made available by Participant prior to termination, subject to extension of required protections under 6(c.)(i).

iii. To the extent the Participation Agreement specifically deals with the return or destruction of PHI following termination or expiration of the Participation Agreement, the provisions of the Participation Agreement shall govern, so long as such provisions are compliant with HIPAA.

## 7. **Miscellaneous**

a. **Regulatory References.** A reference in this Agreement to a section in HIPAA or the Privacy Rule, the Security Standards, or HIPAA Regulations or Guidance means the referenced material as in effect as of the Effective Date or as subsequently amended as supplemented or implemented.

b. **State Privacy or Security Laws.** Business Associate will comply with privacy, data security and consumer notification of a breach of personal information laws of the State of West Virginia (or of the District of Columbia or Maryland or other states, if applicable) to the extent required under the Participation Agreement. In addition, Business Associate will comply with applicable state restrictions on storage or transmission of PHI by Business Associate, as known, or as reasonably should be known, to Business Associate.

c. **Permitted Charges.** To the extent Business Associate takes any action, such as providing information to an Individual under Section 2(g), for which a charge or cost is allowed to be collected under HIPAA or West Virginia law, Business Associate may collect such charge or cost from the Individual or from the PO, as Business Associate determines appropriate in accordance with Business Associate's Policies and Procedures or after discussion with PO.

d. **Other Agreements for Services.** To the extent that Business Associate provides services to PO under agreements other than the Participation Agreement, and such services involve Business Associate's access to, use, creation or maintenance of PHI of PO as a Business Associate under HIPAA ("Other Service Agreements"), unless the Other Service Agreement specifically provides otherwise or incorporates another form of Business Associate Agreement, the provisions of this Agreement shall apply to Business Associate under the Other Service Agreement and all references to Participation Agreement shall be deemed to refer to the Other Service Agreement.

e. **Amendment.** In the event that either party believes that the provisions of this Agreement require amendment based on HIPAA, including but not limited to, Guidance or Regulations or other legislative or regulatory changes to the Privacy Rule or the Security Standards occurring after the Effective Date of this Agreement, that party may notify the other party in writing, including of the text and effective date of the proposed amendment ("Amendment Notice"). The parties shall promptly meet and discuss the

proposed amendment and either agree upon it or agree on other mutually acceptable changes to this Agreement responsive to the Amendment Notice. If the parties are unable to agree on the amendment or such changes, in writing, within thirty (30) days of receipt of the Amendment Notice by the other party, the party providing the Amendment Notice may terminate the Participation Agreement, without cost or penalty, effective on the date on which the proposed amendment was to be effective, as specified in the Amendment Notice.

f. Survival. The respective rights and obligations of the parties under this Agreement which require or contemplate compliance after termination of this Agreement shall survive the termination.

g. Independent Contractor, Not Agent. For purposes of this Agreement and HIPAA, Business Associate will be deemed to be an independent contractor, and not an agent, of PO under applicable law, including federal common law.

h. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits both Business Associate and the PO to comply with the HIPAA, consistent with the Participation Agreement.

[END OF BUSINESS ASSOCIATE AGREEMENT]