

**ATTACHMENT C  
BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (“Agreement”) is entered into by and between the West Virginia Health Information Network (“Business Associate”) and \_\_\_\_\_ (“Participating Organization or PO”).

*Check each applicable box:*

- Full Service
- Data User
- Data Supplier
- WVDirect Subscriber
- WV e-Directive Registry

The PO has checked the box or boxes above that apply to its Participant type with the WVHIN.

**WITNESSETH:**

WHEREAS, the parties to this Business Associate Agreement have entered into a Participation Agreement under which the Business Associate provides certain services to the PO; and

WHEREAS, the PO shall disclose certain information to the Business Associate during the course of the latter’s provision of such services, some of which may constitute “Protected Health Information or PHI” or “Electronic Protected Health Information or ePHI,” as those terms are defined in federal regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), specifically 45 C.F.R. Parts 160 and 164 (the “HIPAA Privacy Rule” and “HIPAA Security Rule”); and

WHEREAS, the Business Associate acknowledges that the Business Associate must comply directly with numerous provisions of the HIPAA Privacy Rule and Security Rule, as both have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”); and

WHEREAS, both the Business Associate and the PO intend to comply with HIPAA and the HITECH Act in order to protect the privacy and to provide for the security of PHI and ePHI disclosed to or created by the Business Associate; and

WHEREAS, both the Business Associate and the PO wish to set forth the terms and the conditions pursuant to which PHI and ePHI received by or created by the Business Associate in the performance of services for the PO shall be handled between themselves and with third parties in compliance with HIPAA and the HITECH Act;

NOW, THEREFORE, in consideration of the mutual promises, covenants, terms, and conditions contained herein, and intending to be legally bound, the Business Associate and the PO agree as follows:

1. Definitions. The following terms shall be defined as set forth below. Terms used, but not defined in this Agreement, shall have the same meaning as those terms in the Privacy Rule, the Security Rule, and the HITECH Act.

(a) “Breach” shall have the same meaning as the term “Breach” is defined at 45 C.F.R. § 164.402, as may be amended, and shall mean the acquisition, access, use, or disclosure of PHI or ePHI in a manner not permitted under the Privacy Rule and in a manner which compromises the security or privacy of the PHI or ePHI, thereby posing a significant risk of financial, reputational, or other harm to an Individual.

(b) For purposes of this Agreement, “Business Associate” shall include the named Business Associate hereinabove.

(c) For purposes of this Agreement, “Covered Entity” shall include the named Covered Entity hereinabove, as well as any other entity specifically identified in any joint Notice of Privacy Practices utilized pursuant to the Privacy Rules.

(d) “Electronic Protected Health Information” or “ePHI” shall have the same meaning as that term is defined at 45 C.F.R. § 160.103, as may be amended, limited to the information received or created by the Business Associate from or on behalf of the Covered Entity.

(e) “HIPAA” shall mean the Health Insurance Portability and Accountability Act of 1996, as may be amended.

(f) “HITECH Act” shall mean the Health Information Technology for Economic and Clinical Health Act, as may be amended.

(g) “Individual” shall have the same meaning as that term is defined at 45 C.F.R. § 160.103, as may be amended, and shall include a person who qualifies as a personal representative of an Individual in accordance with 45 C.F.R. § 164.502(g), as may be amended.

(h) “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information promulgated at 45 C.F.R. Part 160 and Part 164, Subparts A, D, and E, as may be amended, and any other applicable provision of HIPAA, and any amendments thereto, including the HITECH Act.

(i) “Protected Health Information” or “PHI” shall have the same meaning as that term is defined at 45 C.F.R. § 160.103, as may be amended, limited to the information received or created by the Business Associate from or on behalf of the Covered Entity. Unless otherwise stated in this Agreement, any provision, restriction, or obligation in this Agreement related to the use or disclosure of PHI shall apply equally to ePHI.

(j) “Required By Law” shall have the same meaning as that term is defined at 45 C.F.R. § 164.103, as may be amended.

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

(l) “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information promulgated at 45 C.F.R. Part 160 and Part 164, Subpart C, as may be amended, and any other applicable provision of HIPAA, and any amendments thereto, including the HITECH Act.

(m) “Subcontractor” shall mean a subcontractor to the WVHIN other than another Participating Organization.

(n) “Unsecured PHI” shall mean PHI or ePHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued pursuant to § 13402 of the HITECH Act, as provided in 45 C.F.R. § 164.402(2)(iii), as may be amended.

2. Background. The Business Associate is a public-private partnership created by the West Virginia Legislature to develop and operate a statewide Health Information Exchange in West Virginia that provides for the secure exchange of PHI and ePHI. These services have been contracted to the PO, and are more specifically described in a Participation Agreement or a Subscription Agreement between the Business Associate and the PO. In the performance of these services, the PO may disclose PHI to the Business Associate, who may then need to use or disclose such PHI on behalf of the PO. For the purposes of this Agreement, PHI includes only such information that is provided to the Business Associate by the PO. The Business Associate acknowledges that certain sections of the Privacy Rule and the Security Rule, as well as the HITECH Act, apply directly to the Business Associate as they apply to the PO. Both parties are committed to complying with the HIPAA Privacy Rule and HIPAA Security Rule, as amended by the HITECH Act, and accordingly, have entered into this Agreement to set forth the terms and conditions of how such PHI shall be handled between the Business Associate, the PO, and third parties.

3. Permitted Uses and Disclosures by the Business Associate.

(a) Except as otherwise limited in this Agreement, the Business Associate may use or disclose PHI on behalf of the PO for purposes of providing the services described hereinabove and described in any written agreement between the parties, provided that such use or disclosure shall not violate HIPAA, the HITECH Act, the Privacy Rule, or the Security Rule if done by the PO.

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

(c) Except as otherwise limited in this Agreement, the Business Associate may disclose PHI to a Subcontractor for the proper management and administration of the Business Associate, or to carry out the legal responsibilities of the Business Associate, provided that such disclosures are required by law, or that the Business Associate obtains reasonable assurances from the Subcontractor to whom the information is disclosed that it shall remain confidential and may only be used or further disclosed as required by law, or for the purpose for which it was disclosed to the Subcontractor, and the Subcontractor notifies the Business Associate of any instances of which it becomes aware in which the confidentiality of the information has been the subject of a Security Incident or Breach.

(d) Except as otherwise limited in this Agreement, the Business Associate may use PHI to provide data aggregation services to the PO.

(e) The Business Associate may use and disclose PHI only if each such use and disclosure is in compliance with each applicable requirement of 45 C.F.R. § 164.504(e).

(f) The Business Associate may Deidentify any and all PHI that it obtains from the PO, but only if such Deidentification is accomplished in accordance with the requirements of 45 C.F.R. § 164.514(a) and (b).

#### 4. Obligations of the Business Associate.

(a) The Business Associate agrees not to use or disclose PHI other than as permitted or required by this Agreement or as required by law.

(b) The Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. The Business Associate shall implement the administrative, physical, and technical safeguards required for Business Associates by the HIPAA Security Rule in order to protect the confidentiality, integrity, and availability of ePHI that the Business Associate receives, creates, maintains, or transmits.

(c) The Business Associate agrees to notify the PO within thirty (30) days of becoming aware of any use or disclosure of PHI not provided for by this Agreement. In addition, the Business Associate shall notify the PO of any Breach involving Unsecured PHI within thirty (30) days of becoming aware of the Breach. This notice shall include:

(i) the identification of each Patient whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, subject to the Breach;

(ii) a description of what happened, including the date of the Breach and the date of its discovery, if known;

(iii) a description of the types of Unsecured Protected Health Information that were involved in the Breach;

(iv) any steps that Patients should take to protect themselves from potential harm resulting from the Breach; and

(v) a description of what the Business Associate is doing to investigate and mitigate the Breach, and to protect against further Breaches.

The Business Associate agrees to cooperate with the PO in mitigating, to the extent practicable, any harmful effect that is known to exist as a result of such Breach. The Business Associate further agrees to cooperate with the PO in complying with all state and federal public notification requirements arising therefrom.

(d) The Business Associate agrees to ensure that any Subcontractor to whom it provides PHI received from the PO, or created or received by the Business Associate on behalf of the PO, agrees to the same restrictions and conditions that apply in this Agreement to the Business Associate with respect to such information, including but not limited to, the requirement that such Subcontractor implement reasonable and appropriate safeguards to protect such information. The Business Associate shall enter into a written agreement with the Subcontractor which requires the Subcontractor to comply with all of the obligations of the Business Associate under this Agreement.

(e) The Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI received from the PO, or created or received by the Business Associate on behalf of the PO, available to the Secretary for purposes of determining the PO's and/or the Business Associate's compliance with HIPAA, the HITECH Act, the Privacy Rule, or the Security Rule.

(f) If a Patient makes a request to the Business Associate for an accounting of disclosures of his or her PHI, the Business Associate shall forward such request in writing to the PO within ten (10) business days. The PO shall be solely responsible for preparing and delivering the requested accounting to the Patient in accordance with 45 C.F.R. § 164.528. If necessary, the Business Associate shall make available to the PO information about the Business Associate's disclosures of PHI, if any, that must be included to fully and properly respond to the Patient's request for accounting.

(g) If a Patient makes a request to the Business Associate for access to his or her PHI, the Business Associate shall direct the Patient to present any such request for access to the PO within ten (10) business days. The PO shall be solely responsible for making all determinations regarding the grant or denial of a Patient's request for his or her own PHI, and for ultimately providing the requested access in accordance with 45 C.F.R. § 164.524. Any denial of access to the PHI requested by an Individual shall be the sole responsibility of the PO. If necessary, the Business Associate shall make available to the PO any PHI that is maintained by the Business Associate on behalf of the PO to enable the PO to fully and properly respond to the Patient's request for access.

(h) If a Patient makes a request to the Business Associate for amendment of his or her PHI, the Business Associate shall direct the Patient to present any such request for

amendment to the PO within ten (10) business days. The PO shall be solely responsible for making all determinations and taking all actions regarding amendments to PHI in accordance with 45 C.F.R. § 164.526. If necessary, the Business Associate shall include any amendments agreed to by the PO in any PHI that is maintained by the Business Associate on behalf of the PO.

(i) The Business Associate shall rely upon the Minimum Necessary determination of the PO whenever it is necessary to limit the disclosure of PHI to the Minimum Necessary amount in order to accomplish the intended purpose of the request, use, or disclosure.

5. Obligations of the PO.

(a) The PO shall notify the Business Associate of any limitations in the Notice of Privacy Practices maintained by the PO to the extent that such limitations may affect the Business Associate's use or disclosure of the PHI.

(b) The PO shall notify the Business Associate of any changes in, or revocation of, permission granted by a Patient under 45 C.F.R. § 164.506 or § 164.508 to use or disclose PHI, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

(c) The PO shall notify the Business Associate of any restriction to the use or disclosure of PHI that the PO has agreed to in accordance with 45 C.F.R. § 164.522, or in accordance with Section 13405 of the HITECH Act, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI. In addition, the PO shall block the WVHIN's access to any PHI which is the subject of such restriction on use and disclosure.

(d) The PO shall notify Business Associate of any Breach involving Unsecured PHI disclosed through Business Associate's Health Information Exchange within twenty-four (24) hours of becoming aware of the Breach. The notice may be given orally but must also be provided in writing as soon as is reasonably practical, but in no event later than twenty-four (24) hours after discovery. This notification shall include sufficient information to permit Business Associate to begin its investigation process.

(e) The PO shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA, the HITECH Act, the Privacy Rule, or Security Rule if done by the PO.

6. Term.

The term of this Agreement shall be effective on the date that the last of the Business Associate and the PO sign this Agreement, and shall remain in force and effect until terminated pursuant to Section 7 hereinbelow.

7. Termination.

(a) The PO may elect to provide written notice of the material Breach to the Business Associate, after which the Business Associate shall have thirty (30) days to take reasonable steps to cure the Breach. If the Business Associate does not cure the Breach within this specified time, the PO may terminate this Agreement. If neither cure nor termination is feasible, the PO shall report the Breach to the Secretary.

(b) The Business Associate shall not be permitted to terminate this Agreement so long as the services of the Business Associate for and on behalf of the PO are ongoing; provided however, that either party may terminate this Agreement when all of the PHI received from the PO, or created or received by the Business Associate on behalf of the PO, is destroyed or returned to the PO, or if it is infeasible to return or destroy the PHI, the protections are extended to such information in accordance with the provisions of Section 7(c), (d), and (e) hereinbelow.

(c) Upon termination of this Agreement for any reason, the Business Associate shall return or destroy all PHI received and retained by the Business Associate on behalf of the PO. This provision shall apply to PHI that is in the possession of the Business Associate, and of Subcontractors of the Business Associate, and the Business Associate shall so notify its Subcontractors of these obligations. The Business Associate and its Subcontractors shall retain no copies of the PHI.

(d) In the event that the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the PO notification of the conditions that make the return or destruction of such information infeasible. The parties to this Agreement agree, however, that PHI provided to the Business Associate's Health Information Exchange for exchange with another PO may be retained and integrated into the Designated Record Set of other PO. As such, it is not feasible for the Business Associate to return or destroy this PHI upon termination of this Agreement. To the extent that PHI is not returned or destroyed due to the infeasibility of doing so, the Business Associate shall extend the protections of this Agreement to such PHI, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI. Business Associate shall not be responsible for the privacy and security of PHI that may be retained and integrated into the Designated Record Set of another PO.

(e) In the event that it is infeasible for the Business Associate to obtain from a Subcontractor of the Business Associate any PHI in the possession of the Subcontractor, the Business Associate shall provide to the PO notification of the conditions that make return or destruction of such information from the Subcontractor infeasible. Upon such notification, the Business Associate shall require the Subcontractor to extend the protections of this Agreement to such PHI, and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Subcontractor maintains such PHI.

(f) This Agreement shall automatically terminate without any further action of the parties upon the termination of the services provided by the Business Associate to or on behalf of the PO.

8. Statutory or Regulatory References. Any reference in this Agreement to a provision of the HIPAA, the HITECH Act, the HIPAA Privacy Rule or the HIPAA Security Rule shall mean the section as in effect or as amended.

9. Survival. The respective rights and obligations of the Business Associate under Section 7(c), (d), and (e) of this Agreement shall survive the termination of this Agreement.

10. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties, and their respective successors and assigns, any rights, remedies, obligations, or liabilities whatsoever.

11. Amendment. The parties agree to take such action as is necessary to amend this Agreement from time to time in order for the PO to comply with the requirements of HIPAA and the HITECH Act, as those statutes and their implementing regulations may be amended from time to time. The terms and conditions of this Agreement may not be amended, waived, or modified, except as provided in the parties' Participation Agreement or by a writing signed by both parties.

12. Non-Waiver. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any other right or remedy as to any subsequent events.

13. Assignment. Neither party may assign any of its rights or obligations under this Agreement without the prior written consent of the other party.

14. Nature of Agreement. Nothing in this Agreement shall be construed to create a partnership, joint venture, or other joint business relationship between the parties or any of their affiliates, or a relationship of employer and employee between the parties. Rather, it is the intention of the parties that their relationship shall be that of independent contractors.

15. Entire Agreement. This Agreement constitutes the entire agreement between the Business Associate and the PO relating to the matters specified in this Agreement, and supersedes all prior representations or agreements, whether oral or written, with respect to such matters.

16. Severability. Any provision of this Agreement that is determined to be invalid or unenforceable shall be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

17. Notices. All notices, requests, demands, and other communications required or permitted to be given under this Agreement shall be in writing, and shall be effective upon receipt. Such notice may be made by personal delivery, by electronic mail with return electronic mail acknowledging receipt, by courier with tracking capability, or by certified or registered



United States mail, return receipt requested. All such communications shall be sent to the known addresses of the other party. Neither party shall refuse delivery of any notice hereunder.

18. Interpretation. Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA and the HITECH Act, as those statutes and their implementing regulations may be amended from time to time. The provisions of this Agreement shall prevail over any provision of any other agreement between the Business Associate and the PO that may conflict or be inconsistent with any provision in this Agreement.

19. Governing Law. This Agreement and the rights and obligations of the parties hereunder shall be construed, interpreted, and enforced with, and shall be governed by, the laws of the State of West Virginia and the United States of America. The parties consent to the exclusive jurisdiction of the Circuit Court of Kanawha County, West Virginia, to adjudicate any dispute, claim, or cause of action arising hereunder.

20. Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document.

IN WITNESS WHEREOF, the parties have executed this Agreement by their duly authorized representatives to be effective as of the later date written below.

WEST VIRGINIA HEALTH INFORMATION  
NETWORK

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

PARTICIPATING ORGANIZATION

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

