



# WELLRIGHT

## BUSINESS ASSOCIATE ADDENDUM

To the extent Client meets the definition of a “Covered Entity” or “Business Associate” (as those terms are defined in 45 C.F.R. § 160.103), the services provided by WellRight, Inc. (“Vendor”) may involve the use and disclosure of health information that is protected by federal law as defined below (“PHI”). Therefore, Vendor and Client wish to agree to the terms of this **BUSINESS ASSOCIATE ADDENDUM** (“Addendum”) in order to set forth the obligations regarding PHI.

### 1. Definitions.

- Breach. “Breach” shall have the meaning set forth at 45 C.F.R. § 164.402.
- Electronic Health Record. “Electronic Health Record” shall mean an electronic record of health-related information on an Individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.
- Electronic PHI. “Electronic PHI” shall have the same meaning as the term “electronic protected health information” at 45 C.F.R. § 160.103, limited to the information created or received by Vendor from or on behalf of Client.
- HIPAA. “HIPAA” shall mean the Health Insurance Portability and Accountability Act of 1996, as amended, and the implementation regulations thereunder, including without limitation the HITECH Standards (as defined below), and all future regulations promulgated thereunder.
- HIPAA Rules. “HIPAA Rules” means the Privacy Rule (as defined below) and the Security Rule (as defined below).
- HITECH Standards. “HITECH Standards” means Subtitle D of the Health Information Technology for Economic and Clinical Health Act (“HITECH”), found at Title XIII of the American Recovery and Reinvestment Act of 2009, and any regulations promulgated thereunder, including all amendments to the HIPAA Rules.
- Individual. “Individual” shall have the same meaning as the term “individual” at 45 C.F.R. § 160.103, and any amendments thereto, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- Privacy Rule. “Privacy Rule” means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164.

- Protected Health Information. “Protected Health Information” or “PHI” shall have the same meaning as the term “protected health information” at 45 C.F.R. § 160.103, and any amendments thereto, limited to the information created or received by Vendor from or on behalf of Client.
- Required By Law. “Required By Law” shall have the same meaning as the term “required by law” at 45 C.F.R. § 164.103.
- Secretary. “Secretary” shall mean the Secretary of the United States Department of Health and Human Services or his/her designee.
- Security Incident. “Security Incident” shall have the same meaning as the term “security incident” at 45 C.F.R. § 164.304.
- Security Rule. “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160, 162, and 164.
- Unsecured PHI. “Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in accordance with the HITECH Standards.
- Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy Rule, the Security Rule, the HITECH Standards or any future regulations promulgated or guidance issued by the Secretary thereunder.

2. Obligations and Activities of Vendor.

- a) Vendor agrees to not use or disclose PHI other than as permitted or required by this Addendum, the Agreement or any other underlying agreement between the Parties or as Required By Law.
- b) Vendor will make reasonable efforts to the extent practicable, to limit requests for and the use and disclosure of PHI to a Limited Data Set (as defined in 45 C.F.R. § 164.514(e)(2)) or, if needed by Vendor, to the minimum necessary PHI to accomplish the intended purpose of such use, disclosure or request, and as applicable, in accordance with the regulations and guidance issued by the Secretary on what constitutes the minimum necessary for Vendor to perform its obligations to Client under this Addendum or as Required By Law.
- c) Vendor agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Addendum, including the implementation of administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic PHI that it creates, receives, maintains or transmits on behalf of Client. Vendor shall abide by the Security Standards for the Protection of Electronic PHI at 45 C.F.R. Part 164, Subpart C, including the Administrative Safeguards at 45 C.F.R. § 164.308, the Physical Safeguards at 45 C.F.R. § 164.310, the Technical Safeguards at 45 C.F.R.

§ 164.312, and the policies and procedures and documentation requirements at 45 C.F.R. § 164.316, to the same extent such provisions apply to Client.

- d) Vendor agrees to mitigate, to the extent practicable, any harmful effect that is known to Vendor of a use or disclosure of PHI by Vendor in violation of the requirements of this Addendum.
- e) Vendor agrees to report to Client any use or disclosure of the PHI not provided for by this Addendum of which it becomes aware. To the extent that Vendor creates, receives, maintains or transmits Electronic PHI, Vendor agrees to report promptly to Client any Security Incident, as determined by Vendor, involving PHI of which Vendor becomes aware. Vendor hereby notifies Client of the ongoing existence and occurrence of attempted but unsuccessful Security Incidents and Client acknowledges and agrees that no additional notification to Client of such unsuccessful Security Incidents is required.
- f) Following Vendor's discovery of a use or disclosure of Unsecured PHI that is not provided for by this Addendum, Vendor shall promptly perform a risk assessment to determine whether the use or disclosure qualifies as a Breach. Following such risk assessment, Vendor shall notify Client of the Breach without unreasonable delay, and in no event later than seven (7) calendar days after Vendor, or any of its employees or agents, discovered the Breach. Such notification shall include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Vendor to have been, accessed, acquired, used, or disclosed during the Breach and any other information available to Vendor about the Breach which is required to be included in the notification of the Breach provided to the Individual in accordance with 45 C.F.R. §164.404(c). A Breach of Unsecured PHI shall be treated as discovered as of the first day on which such Breach is known to Vendor or should have been known to Vendor by exercising reasonable diligence.
- g) Vendor agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Vendor on behalf of Client, agrees in writing to the same restrictions and conditions that apply through this Addendum to Vendor with respect to such information. Moreover, Vendor agrees to ensure any such agent or subcontractor agrees to implement reasonable and appropriate safeguards to protect Electronic PHI.
- h) Vendor agrees to provide access, at the request of Client, and in a time and manner mutually acceptable to Vendor and Client to PHI in a Designated Record Set, to Client, or as directed by Client, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524.
- i) Vendor agrees to make any amendment(s) to PHI in its possession contained in a Designated Record Set that Client directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Client, and in the time and manner mutually acceptable to Vendor and Client.

- j) Vendor agrees to document such disclosures of PHI and information related to such disclosures as would be required for Client to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.
- k) Within ten (10) business days (or such other date that Vendor and Client may reasonably agree upon) of receiving written notice from Client that Client has received a request for an accounting of disclosures of PHI from an Individual, Vendor agrees to provide to Client information collected to permit Vendor to make the accounting required in accordance with 45 C.F.R. § 164.528.
- l) Vendor agrees to make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Vendor on behalf of, Client, available to the Secretary for purposes of determining Client's compliance with the Privacy Rule.
- m) To the extent Vendor is delegated to carry out Client's obligations under the Privacy Rule, Vendor shall comply with the requirements of the Privacy Rule that apply to Client in the performance of such delegated obligations.
- n) The Parties agree that the HITECH Standards that are applicable to Client shall also be applicable to Vendor and are hereby incorporated herein by reference. In the event the Secretary issues regulations that require specific modifications to this Addendum related to these provisions, the Parties agree to take such action as is necessary to amend this Addendum to meet such requirements

3. General Use and Disclosure Provisions.

Except as otherwise limited in this Addendum,

- a) Vendor reserves the right to **use** PHI for the proper management and administration of Vendor, to carry out the legal responsibilities of Vendor, or to provide data aggregation services relating to the health care operations of a Client.
- b) Vendor may **use or disclose** PHI to perform functions, activities, or services for, or on behalf of, Client provided that such use or disclosure would not violate the Privacy Rule if done by Client.
- c) Vendor may **disclose** PHI in its possession for the proper management and administration of Vendor, provided that disclosures are Required by Law, or Vendor obtains reasonable assurances from the third party to whom the information is disclosed that such PHI will be held confidentially and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the third party, and the third party notifies Vendor of any instances of which it is aware in which the confidentiality of the PHI has been breached.

4. Term and Termination.

- a) Term. The term of this Addendum shall commence on the Effective Date and shall terminate automatically upon termination of the Agreement unless terminated

earlier, as provided below, or unless the terms of this Addendum are extended in writing by the Parties.

- b) Termination for Cause. Upon either party's knowledge of a material breach by the other party of this Addendum, the non-breaching party shall either:
  - i) Provide an opportunity for the breaching party to cure the breach or end the violation and terminate this Addendum if the breaching party does not cure the breach or end the violation within the time specified by the non-breaching party; or
  - ii) Immediately terminate this Addendum if the non-breaching party has breached a material term of this Addendum and cure is not possible.
- c) Effect of Termination.
  - i) Except as provided in paragraph (ii) of this Section, upon termination of this Addendum, for any reason, Vendor shall return or destroy all PHI received from Client, or created or received by Vendor on behalf of Client. This provision shall apply to PHI that is in the possession of subcontractors or agents of Vendor. Vendor shall not retain copies of the PHI.
  - ii) In the event that returning or destroying the PHI is not feasible, Vendor shall provide to Client notification of the conditions that make return or destruction not feasible. Upon determination that return or destruction of PHI is not feasible, Vendor shall extend the protections of this Addendum to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction not feasible, for so long as Vendor maintains such PHI.

5. Miscellaneous.

- a) Regulatory References. A reference in this Addendum to a section in the Privacy Rule or the Security Rule means the section as in effect or as amended, and for which compliance is required.
- b) Amendment. No change, amendment, or modification of this Addendum shall be valid unless set forth in writing and agreed to by both Parties. Notwithstanding the foregoing, the Parties acknowledge that state and federal laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to ensure compliance with such developments. The Parties specifically agree to take such action as may be necessary from time to time as is necessary for the Parties to comply with the requirements of HIPAA.
- c) Survival. The respective rights and obligations of Vendor under Section 4 of this Addendum shall survive the termination of this Addendum, unless expressly stated otherwise.

- d) Interpretation. Any ambiguity in this Addendum shall be resolved to permit Vendor and Client to comply with HIPAA. To the extent any term of this Addendum conflicts with or is contrary to a term in the Agreement, this Addendum shall govern.
- e) Notice. Any notice, report or other communication required under this Addendum shall be made in accordance with the Agreement.
- f) Governing Law. Notwithstanding any provision of the Agreement, the rights, duties and obligations of the Parties to this Addendum and the validity, interpretation, performance and legal effect of this Addendum shall be governed and determined by applicable federal law with respect to the Privacy Rule and the Security Rule and otherwise by the laws of the State of Illinois.