



BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is made and entered into on this ____day of _____, 20____ (the "Effective Date") by and between _____ ("Covered Entity"), and Illuma Care Connections, LLC. ("Business Associate"). Covered Entity and Business Associate are sometimes referred to herein collectively as the "parties" and individually as a "party".

WHEREAS, Business Associate performs certain functions on behalf of and/or provides certain services that qualify it as a "business associate" of Covered Entity pursuant to 45 C.F.R. § 160.103;

WHEREAS, in the performance of such functions and/or the provision of such services, Business Associate may require access to Protected Health Information (defined below) in possession, custody, or control of Covered Entity, or may create or receive Protected Health information on behalf of Covered Entity for the limited purposes identified in this Agreement;

WHEREAS, pursuant to the Federal Standards for Privacy and Security of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, as established under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Covered Entity cannot disclose Protected Health Information to or authorize the creation or receipt of Protected Health Information on its behalf by Business Associate unless Covered Entity obtains from Business Associate satisfactory assurances that Business Associate will properly safeguard such information; and

WHEREAS, Business Associate is willing to provide such assurances to Covered Entity under the terms specified herein.

NOW, THEREFORE, the parties agree as follows:

DEFINITIONS.

- (a) *Breach*. "Breach" shall have the same meaning as the term "breach" in 45 C.F.R. § 164.402.
- (b) *Electronic Health Record*. "Electronic Health Record" shall have the same meaning as the term "electronic health record" in American Recovery and Reinvestment Act of 2009, § 13400(5).
- (c) *Electronic Protected Health Information*. "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103.
- (d) *Electronic Transactions Rule*. "Electronic Transactions Rule" shall mean the regulations issued by HHS concerning standard transactions and code sets under 45 C.F.R. Parts 160 and 162.
- (e) *HHS*. "HHS" shall mean the Department of Health and Human Services.
- (f) *Privacy Rule*. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, subparts A and E.
- (g) *Protected Health Information*. "Protected Health Information" shall have the same meaning as the term



"protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(h) *Required By Law*. "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

(i) *Security Incident*. "Security Incident" shall have the same meaning as the term "security incident" in 45 C.F.R. § 164.304.

(j) *Security Rule*. "Security Rule" shall mean the Security Standards and Implementation Specifications at 45 C.F.R. Parts 160 and 164, subpart C.

(k) *Subcontractor*. "Subcontractor" shall have the same meaning as the term "Subcontractor" in 45 C.F.R. § 164.103.

(l) *Transaction*. "Transaction" shall have the meaning given the term "transaction" in 45 C.F.R. § 160.103.

(m) *Unsecured Protected Health Information*. "Unsecured protected health information" shall have the meaning given the term "unsecured protected health information" in 45 C.F.R. § 164.402.

I. SAFEGUARDING PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION

(a) **Permitted Uses and Disclosures**. Business Associate is permitted to use and disclose Protected Health Information only as set forth below:

(i) **Functions and Activities on Covered Entity's Behalf**. To perform functions on behalf of Covered Entity as such functions are agreed upon by Covered Entity and Business Associate pursuant to an underlying agreement between the parties (the "Services Use Agreement").

(ii) **Business Associate's Operations**. For Business Associate's proper management and administration or to carry out Business Associate's legal responsibilities, provided that, with respect to disclosure of the Protected Health Information, either:

(A) The disclosure is Required by Law; or

(B) Business Associate obtains reasonable assurance from any other person or entity to which Business Associate will disclose Covered Entity's Protected Health Information that the person or entity will:

(1) Hold the Protected Health Information in confidence and use or further disclose the Protected Health Information only for the purpose for which Business Associate disclosed the Protected Health Information to the person or entity or as Required by Law; and

(2) Promptly notify Business Associate of any instance of which the person or entity becomes aware in which the confidentiality of the Protected Health Information was breached.



- (iii) **Minimum Necessary.** Business Associate will, in its performance of the functions, activities, services, and operations specified above, make reasonable efforts to use, to disclose, and to request only the minimum amount of the Protected Health Information reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that Business Associate will not be obligated to comply with this minimum-necessary limitation of 45 C.F.R. § 164.502(b) if neither Business Associate nor Covered Entity is required to limit its use, disclosure or request to the minimum necessary. Business Associate and Covered Entity acknowledge that the phrase "minimum necessary" shall be interpreted in accordance with 45 C.F.R. § 164.502(b).

- (iv) **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 the Protected Health Information by Business Associate in violation of the requirements of this Agreement and to assist Covered Entity's efforts to mitigate any such harmful effect.

- (b) **Required Uses and Disclosures.** Business Associate shall disclose Protected Health Information (i) when required by the Secretary of DHHS under 45 C.F.R. Part 160, Subpart C to investigate or determine Business Associate's compliance with Subchapter C of 45 C.F.R., Subtitle A, and (ii) to Covered Entity, the individual or the individual's designee, as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524(c)(2)(ii) and (3)(ii) with respect to the individual's request for an electronic copy of his or her Protected Health Information.

- (c) **Prohibition on Unauthorized Use or Disclosure.** Business Associate will neither use nor disclose the Protected Health Information, except as permitted or required by this Agreement or in writing by Covered Entity or as Required by Law. This Agreement does not authorize Business Associate to use or disclose the Protected Health Information in a manner that will violate the Privacy Rule.

- (d) **Information Safeguards.**
 - (i) **Privacy of Protected Health Information.** Business Associate will comply with the Privacy Rule to the extent applicable to Business Associate. The Business Associate's Privacy Rule safeguards must reasonably protect the Protected Health Information from any intentional or unintentional use, access or disclosure in violation of the Privacy Rule and limit incidental use, access or disclosure made pursuant to a use, access or disclosure otherwise permitted by this Agreement.
 - (ii) **Security of Electronic Protected Health Information.** Business Associate will comply with the Security Rule and will use appropriate administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that Business Associate creates, receives, maintains, or transmits on Covered Entity's behalf as required by the Security Rule. Business Associate shall review and modify the security measures implemented in accordance with the above as needed to continue provision of reasonable and appropriate protection of Electronic Protected Health Information. Business Associate shall update documentation of such security measures in accordance with 45 C.F.R. § 164.316(b) (2) (iii) and shall designate a Security Officer and undertake appropriate training of its personnel in accordance with the Security Rule.

- (e) **Subcontractors and Agents.** Business Associate will ensure that any of its Subcontractors and agents, to whom it provides Protected Health Information and/or Electronic Protected Health Information received from, or created or received by the Business Associate on behalf of, the Covered Entity agree to the same restrictions and conditions that apply to the Business Associate with respect to such information. Business Associate may permit a business associate that is a Subcontractor to create, receive, maintain, or transmit Electronic Protected Health Information on its behalf only if Business Associate obtains satisfactory assurances, in accordance with 45 C.F.R. § 164.314(a), that the Subcontractor will appropriately safeguard such information. Business Associate agrees that any of Business Associate's Subcontractors that create, receive, maintain or transmit Protected Health Information or Electronic Protected Health Information on behalf of Business Associate shall comply with the applicable requirements of 45 C.F.R. Part 164, Subpart C by entering into a contract or other arrangement



with such Subcontractor that complies with 45 C.F.R. § 164.314(a) (2) (i).

- (f) **Prohibition on Sale of Records.** Business Associate shall not engage in any sale of Protected Health Information as defined in 45 C.F.R. § 164.501.

II. COMPLIANCE WITH SECURITY STANDARDS. If Business Associate conducts in whole or part electronic transactions on behalf of Covered Entity for which HHS has established standards, Business Associate shall comply, and will require any Subcontractor it involves with the conduct of such transactions to comply, with each applicable requirement of security standards set forth at 45 C.F.R. § 164.302 et seq. Business Associate shall also comply with the national provider identifier requirements, if and to the extent applicable.

III. INDIVIDUAL RIGHTS.

- (a) **Access.** Business Associate will make available Protected Health Information in accordance with 45 C.F.R. § 164.524, upon request from Covered Entity, so that Covered Entity may meet its access obligations under 45 C.F.R. § 164.524. Effective September 23, 2013, if the Protected Health Information is maintained electronically in a designated record set in the Business Associate's custody or control, then the Covered Entity shall have a right to obtain from Business Associate a copy of such information in an electronic format.
- (b) **Amendment.** Business Associate will, upon receipt of written notice from Covered Entity, promptly amend or permit Covered Entity access to amend any portion of an individual's Protected Health Information that is in a designated record set in the custody or control of the Business Associate, so that Covered Entity may meet its amendment obligations under 45 C.F.R. § 164.526.
- (c) **Disclosure Accounting.** Business Associate will make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528, upon request from Covered Entity, to allow Covered Entity to meet its disclosure accounting obligations under 45 C.F.R. § 164.528. Business Associate will maintain the Disclosure Information for six (6) years following the date of the accountable disclosure to which the Disclosure Information relates.
- (d) **Restriction Agreements and Confidential Communications.** Business Associate will comply with any agreement that Covered Entity makes that either (i) restricts use, access or disclosure of Covered Entity's Protected Health Information pursuant to 45 C.F.R. § 164.522(a), or (ii) requires confidential communication about Covered Entity's Protected Health Information pursuant to 45 C.F.R. § 164.522(b), provided that Covered Entity notifies Business Associate in writing of the restriction or confidential communication obligations that Business Associate must follow. Covered Entity will promptly notify Business Associate in writing of the termination of any such restriction agreement or confidential communication requirement and, with respect to termination of any such restriction agreement, instruct Business Associate whether any of Covered Entity's Protected Health Information will remain subject to the terms of the restriction agreement.

IV. REPORTING.

- (a) **Breach.** Business Associate will report to Covered Entity any Breach of Unsecured Protected Health Information as soon as reasonably practicable and not more than five (5) calendar days after discovery of such Breach. Business Associate will treat a Breach as being discovered in accordance with 45 C.F.R. § 164.410. Business Associate will make the report to Covered Entity's Privacy Officer. If a delay is requested by a law-enforcement official in accordance with 45 C.F.R. § 164.412, Business Associate may delay notifying Covered Entity for the applicable time period. Business Associate's report will include at



least the following, provided that absence of any information will not be cause for Business Associate to delay the report:

- (i) Identify the nature of the Breach;
- (ii) Identify the types of Unsecured Protected Health Information used, accessed or disclosed during such Breach;
- (iii) Identify what corrective action Business Associate or its Subcontractors took or will take to prevent further Breaches or other non-permitted or violating uses, accesses or disclosures;
- (iv) Identify what Business Associate or its Subcontractors did or will do to mitigate any harmful effect of the Breach; and
- (v) Provide such other information that Covered Entity is required to include in notification to the individual whose information is the subject of such Breach, as required by 45 C.F.R. § 164.410.

(b) **Security Incidents.** Business Associate will provide notice to Covered Entity of any Security Incident of which Business Associate becomes aware. Business Associate will make the report in the form noted in Section V.(a) above and will cooperate with Covered Entity to promptly address and correct the Security Incident.

(c) **Notice.** Notices required to be given pursuant to this Agreement shall be deemed given when properly addressed to a party's privacy contact upon the date of receipt if hand-delivered or emailed, or three (3) business days after deposit in the U.S. mail if mailed by registered or certified mail, postage prepaid, or one (1) business day after deposit with a national overnight courier for next business day delivery, or upon the date of electronic confirmation of receipt of a facsimile transmission.

(d) **Address for Notice.** Notice shall be communicated:

If to Covered Entity:

Contact Office: _____

Contact Signature: _____

Telephone: _____

Email: _____

