



Business Associate Agreement

This Business Associate Agreement (the “Agreement”) is entered into as of _____, (the “Effective Date”) by and between Outcomes Operating, Inc. together with its subsidiaries and affiliates (“Outcomes” or “Business Associate”) and _____ (“Customer” or “Covered Entity”). Outcomes and Customer may sometimes be referred to herein as a “Party” or collectively as the “Parties.”

WHEREAS, Outcomes is in the business of producing, selling, installing, and supporting pharmacy software, and in the normal course of installation and support of said software will, from time to time, have access to protected health information;

WHEREAS, Customer is in the business of providing pharmacy services, Customer desires to purchase software and/or services from Outcomes, and Customer acknowledges Outcomes' need for occasional access to protected health information in the furtherance of its services to Customer;

WHEREAS, Outcomes is a Business Associate (as defined below) for the purposes of Customer;

WHEREAS, Outcomes and Customer maintain a separate Underlying Services Agreement (as defined herein);

WHEREAS, Outcomes and Customer wish to enter into this Agreement to confirm their compliance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), including the HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164; the HIPAA Security Rule, 45 C.F.R. Parts 160, 162 and 164; the Act; the Breach Notification Rule (8/24/09), 45 C.F.R. Parts 160 and 164; Subtitle D of the American Recovery and Reinvestment Act of 2009 (“ARRA '09”) entitled "Health Information Technology for Economic and Clinical Health", generally referred to as the HITECH Act (“HITECH”), Section 13400 *et seq.*; state laws and regulations not preempted by HIPAA that are addressed to the privacy and security of Protected Health Information (“PHI”); and

WHEREAS, the purpose of this Agreement is to reflect the intention of the Parties that their relationship shall be in compliance with the applicable statutes, rules and regulations referenced herein.

NOW, THEREFORE, in consideration of the foregoing premises and the mutual covenants and agreements contained herein, and intending to be legally bound hereby, the Parties hereto agree as follows:

1. Definitions

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 C.F.R §160.103, 45 CFR § 164.304, and 45 C.F.R. § 164.501.

- 1.1 **Business Associate**. “Business Associate” shall have the same meaning as the term “business associate” in 45 C.F.R §160.103, and for the purposes of this Agreement shall mean Outcomes.
- 1.2 **Covered Entity**. “Covered Entity” shall have the same meaning as the term “covered entity” in 45 C.F.R § 160.103, and for the purposes of this Agreement shall mean Customer.

- 1.3 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, and shall refer to PHI that Customer, or Business Associate on behalf of Customer, transmits or maintains in electronic media.
- 1.4 Individual. “Individual” shall have the same meaning as the term “individual” in 45 C.F.R. § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502.
- 1.5 Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.
- 1.6 Protected Health Information. “Protected Health Information” shall have the same meaning as the term "protected health information" in 45 C.F.R. § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- 1.7 Underlying Services Agreement. “Underlying Services Agreement” shall mean the agreement between the Parties hereto setting forth the scope of the services Customer has engaged Business Associate to provide on Customer’s behalf.
- 1.8 Unsecured Protected Health Information. “Unsecured Protected Health Information” or “Unsecured PHI” shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance, as set forth as 45 C.F.R. § 164.402.
- 1.9 Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.501.
- 1.10 Secretary. “Secretary” shall refer to the U.S. Secretary of Health and Human Services.

2. Obligations and Activities of Business Associate

- 2.1 Obligations Regarding Uses and Disclosures of PHI
 - a) Outcomes agrees to not use or further disclose Protected Health Information other than as permitted or required by the Underlying Services Agreement or as Required by Law.
 - b) Outcomes agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
 - c) Outcomes agrees to mitigate, to the extent practicable, any harmful effect that is known to Outcomes of a use or disclosure of Protected Health Information by Outcomes in violation of the requirements of this Agreement.
 - d) Outcomes agrees to report to Customer any use or disclosure of the Protected Health Information not provided for by this Agreement.
 - e) Outcomes agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from Customer, or created by

Outcomes on behalf of Customer, agrees to the same restrictions and conditions that apply through this Agreement to Outcomes with respect to such information.

- f) Outcomes agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Outcomes on behalf of Customer, available to Customer, or at the request of the Customer to the Secretary, in a time and manner designated by the Customer or the Secretary, for purposes of the Secretary determining Customer's compliance with the Privacy Rule.
- g) Outcomes agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Customer to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.
- h) Outcomes agrees to provide to Customer or an Individual, in the reasonable time and manner designated by Customer, information collected in accordance with Section 2.7 of this Agreement, to permit Customer to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.
- i) Outcomes agrees, at the Customer's request, to provide to Customer or an Individual in the reasonable time and manner designated by Customer, the Protected Health Information requested by an individual pursuant to 45 C.F.R. § 164.524.
- j) Outcomes agrees, at the Customer's request, and in the reasonable time and manner designated by Customer, to provide to Customer the Protected Health Information that an individual seeks to amend pursuant to 45 C.F.R. § 164.526.

2.2 Obligations Regarding Electronic PHI

- a) Outcomes agrees to comply with the HIPAA Security Regulations, 45 C.F.R. Parts 160, 162 and 164, with respect to any electronic PHI Outcomes creates, receives, maintains or transmits for or on behalf of Customer.
- b) In particular, with respect to such electronic PHI:
 - (i) Outcomes agrees to implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI as required by the Security Regulations.
 - (ii) Outcomes will ensure that any agent, including a subcontractor to whom it provides electronic PHI, agrees to implement reasonable and appropriate safeguards to protect the electronic PHI.
 - (iii) Outcomes shall report to Customer any successful security incident of which Business Associate becomes aware with respect to the electronic PHI. Notwithstanding the foregoing, the Parties acknowledge and agree that this Section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined herein) for which no additional notice to Covered Entity

shall be required. “Unsuccessful Security Incidents” shall include, but not be limited to, pings and other broadcast attacks on Business Associate’s firewall, port scans, unsuccessful log-on attempts, phishing attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

2.3 Obligations Regarding Notification of Breaches of Unsecured PHI.

- a) Outcomes will notify Customer of Breaches of Unsecured PHI without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of such a Breach in Unsecured PHI, as these terms are defined at 45 C.F.R. 164 subpart D. Outcomes notice to the Customer shall include the applicable elements as set forth at 45 C.F.R. §164.410.
- b) Comply with all requirements of the HIPAA Breach Notification Rule pursuant to 45 C.F.R. 164 subpart D.

3. Permitted Uses and Disclosures by Business Associate

- 3.1. Except as otherwise limited in this Agreement, Outcomes may use or disclose Protected Health Information on behalf of, or to provide services to, Customer provided that such use or disclosure of Protected Health Information is: (A) in furtherance of the purposes set forth in the Underlying Services Agreement, including, but not limited to, the Installation and/ or Support of Outcomes' software, and associated licensed software; and (B) if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Customer.
- 3.2. Except as otherwise limited in this Agreement, Outcomes may disclose Protected Health Information for the proper management and administration of Outcomes, provided that any such disclosures are either: (A) required by law; or (B) made after Outcomes 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 Outcomes of any instances of which it is aware in which the confidentiality of the information has been breached.
- 3.3. Outcomes may provide data aggregation services relating to the health care operations of the Customer pursuant to 45 CFR § 164.504(e)(2)(i)(B).
- 3.4. Business Associate may use PHI to create de-identified information (“De-Identified Information”) in accordance with the applicable provisions of 45 C.F.R. § 164.514, and may use and disclose such De-Identified Information: (1) for the purposes described in the Underlying Services Agreement between Covered Entity and Business Associate; and (2) to fulfill any legal responsibilities of Covered Entity and/or Business Associate. Business Associate may also use and disclose such De-Identified Information for any purpose and in any manner consistent with applicable law; provided, however, that: (1) Business Associate will not re-identify De-Identified Information and (2) Business Associate will take reasonable steps to ensure that its workforce and any Subcontractors or third parties that receive De-Identified Information do not re-identify De-Identified Information.

4. Covered Entity Obligations

- 4.1 Customer shall not request Outcomes to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Customer.
- 4.2 Customer shall notify Business Associate of any restriction to the use or disclosure of PHI that Customer has agreed to in accordance with 45 C.F.R. § 164.522, or as mandated pursuant to Section 13405(c) of HITECH, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

5. Term and Termination

- 5.1. Term. The Term of this Agreement shall commence as of the Effective Date and shall terminate when all of the Protected Health Information provided by Customer to Outcomes, or created or received by Outcomes on behalf of Customer, is destroyed or returned to Customer, or, if Business Associate determines 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.
- 5.2. Termination for Cause. Upon either Party's knowledge of a material breach by the other Party, the non-breaching Party shall provide an opportunity for the breaching Party to cure the breach or end the violation. If the breaching Party does not cure the breach or end the violation within the reasonable time specified by the non-breaching Party, or if the breaching Party has breached a material term of this Agreement and cure is not possible, the non-breaching Party may immediately terminate this Agreement. If neither termination nor cure is feasible, the non-breaching Party may report the violation to the Secretary.
- 5.3. Effect of Termination.
 - a) Except as provided in paragraph (b) of this section, upon termination of this Agreement, for any reason, Outcomes shall return or destroy all Protected Health Information received from Customer, or created or received by Outcomes on behalf of Customer. This provision also shall apply to Protected Health Information that is in the possession of subcontractors or agents of Outcomes. Outcomes shall retain no copies of the Protected Health Information.
 - b) In the event that Outcomes determines that returning or destroying the Protected Health Information is infeasible, Outcomes shall provide to Customer, notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Outcomes shall extend the protections of this 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 Outcomes maintains such Protected Health Information.

6. Other Terms

- 6.1. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Customer to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.

- 6.2. Survival. The respective rights and obligations of Outcomes under Section 5.3 of this Agreement shall survive the termination of this Agreement.
- 6.3. Interpretation. The provisions of this Agreement are to be interpreted at all times so as to be consistent with the statutes, rules and regulations referred to in this Agreement. In the event of any conflict among the provisions of this Agreement and the statutes, rules and regulations referred to herein, the provisions of such statutes, rules and regulations as currently written or as hereafter amended or otherwise modified by the Secretary shall prevail. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Parties to comply with HIPAA.
- 6.4. Entire Agreement. This Agreement contains all of the agreements and understandings between the parties with respect to the subject matter hereof. No agreement or other understanding in anyway modifying the terms hereof will be binding unless made in writing as a modification or amendment to this Agreement and executed by both parties.
- 6.5. Conflicts. In the event of a conflict between the terms of this Agreement and other terms of the Underlying Services Agreement, the terms of this Agreement shall govern and control.

[Signature page follows.]

IN WITNESS WHEREOF, Outcomes and Customer agree to and intend to be legally bound by all terms and conditions set forth above and hereby execute this Agreement as of the Effective Date.

Outcomes Operating, Inc.:

Customer:

By: _____

By: _____

Name: John Schaefer

Name: _____

Title: Chief Legal Officer

Title: _____