

# BUSINESS ASSOCIATE NON-DISCLOSURE AGREEMENT

This HIPAA Business Associate Agreement (this "Agreement") is entered into and made effective as of (the "Effective Date"), by and between **[COVERED ENTITY NAME HIPAA]**, a Corporation of the State of [STATE], with an address of [FIRST PARTY ADDRESS] (the "Covered Entity"), and **[SECOND PARTY NAME]**, a Individual organized under the laws of the State of [STATE], with an address of [SECOND PARTY ADDRESS] (the "Business Associate").

## Recitals

WHEREAS, Covered Entity is a "covered entity" and Business Associate is a "business associate" as those terms are defined under the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the implementing regulations at 45 C.F.R. Parts 160 and 164 (collectively, the "HIPAA Rules");

WHEREAS, Covered Entity wishes to disclose certain Protected Health Information ("PHI") to Business Associate, and Business Associate will create, receive, maintain, or transmit PHI on behalf of Covered Entity, in connection with the services described below; and

WHEREAS, the HIPAA Rules at 45 C.F.R. §164.504(e) require Covered Entity to obtain satisfactory assurances, in the form of a written agreement, that Business Associate will appropriately safeguard PHI;

NOW, THEREFORE, in consideration of the mutual covenants and other good and valuable consideration, the Parties agree as follows.

## 1. Definitions

Capitalized terms used but not defined in this Agreement have the meanings set forth in the HIPAA Rules, including: "Breach," "Designated Record Set," "Electronic Protected Health Information" (ePHI), "Health Care Operations," "Individual," "Protected Health Information," "Required By Law," "Secretary," "Security Incident," "Subcontractor," "Unsecured Protected Health Information," and "Use."

## 2. Services; Purpose

Business Associate will perform the following services involving the creation, receipt, maintenance, or transmission of PHI on behalf of Covered Entity: **[SERVICES PERFORMED BY THE BUSINESS ASSOCIATE]** (the "Services"). The purpose of this Agreement is: **[BUSINESS PURPOSE]** (the "Purpose").

### **3. Permitted Uses and Disclosures**

Business Associate shall Use or Disclose PHI only: (a) as necessary to perform the Services described above and consistent with Covered Entity's minimum-necessary policies; (b) as Required By Law; (c) for Business Associate's proper management and administration or to carry out its legal responsibilities, provided any disclosure to a third party is Required By Law or is made under a written agreement providing at least the same protections and requiring the recipient to notify Business Associate of any breach; (d) to provide Data Aggregation services relating to Covered Entity's Health Care Operations if permitted by the Services; or (e) as otherwise permitted by 45 C.F.R. §164.504(e) and §164.502. Business Associate shall not Use or Disclose PHI in any manner that would violate the HIPAA Rules if done by Covered Entity.

### **4. Minimum Necessary**

Business Associate shall make reasonable efforts to Use, Disclose, and request only the minimum amount of PHI necessary to accomplish the intended purpose, consistent with 45 C.F.R. §164.502(b) and Covered Entity's policies.

### **5. Safeguards**

Business Associate shall implement and maintain appropriate administrative, physical, and technical safeguards, and shall comply with the Security Rule at 45 C.F.R. Part 164, Subpart C, with respect to ePHI. Business Associate shall conduct a risk analysis, implement a risk-management program, maintain written policies and procedures, train its workforce, and document compliance as required by the HIPAA Rules.

### **6. Reporting; Breach Notification**

Business Associate shall report to Covered Entity any Use or Disclosure of PHI not permitted by this Agreement, any Security Incident (45 C.F.R. §164.304), and any Breach of Unsecured PHI (45 C.F.R. §164.402), without unreasonable delay and in no event later than **15 days** after discovery. The report shall include, to the extent available, the information required by 45 C.F.R. §164.410(c), including identification of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, Used, or Disclosed, a description of the nature of the Breach, the types of information involved, mitigation steps, and corrective actions.

### **7. Subcontractors**

Business Associate may engage Subcontractors that create, receive, maintain, or transmit PHI on its behalf, provided that Business Associate first obtains satisfactory written assurances, through a written agreement that complies with 45 C.F.R. §164.502(e)(1)(ii) and §164.504(e)(5), that the Subcontractor will

protect PHI on terms at least as restrictive as those in this Agreement. Business Associate remains responsible for its Subcontractors' compliance.

## **8. Individual Rights**

Within fifteen (15) business days after a request by Covered Entity, Business Associate shall: (a) make PHI in a Designated Record Set available to Covered Entity (or, as directed by Covered Entity, to an Individual) under 45 C.F.R. §164.524; (b) make amendments to PHI in a Designated Record Set and incorporate them as directed by Covered Entity under 45 C.F.R. §164.526; and (c) provide an accounting of disclosures under 45 C.F.R. §164.528. Business Associate shall document such disclosures in the manner required for Covered Entity's accounting obligations.

## **9. Access by HHS**

Business Associate shall make its internal practices, books, and records, including policies and procedures and PHI, relating to the Use and Disclosure of PHI received from or created or received on behalf of Covered Entity, available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with the HIPAA Rules.

## **10. Mitigation**

Business Associate shall mitigate, to the extent practicable, any harmful effect known to Business Associate of a Use or Disclosure of PHI in violation of this Agreement.

## **11. Return or Destruction of PHI**

Upon termination of this Agreement, Business Associate shall, if feasible, return or destroy all PHI received from, or created or received on behalf of, Covered Entity, and retain no copies in any form. Business Associate shall ensure that any Subcontractor does the same. If return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to the PHI, limit further Uses and Disclosures to those purposes that make return or destruction infeasible, and continue to comply with this Agreement for as long as it retains such PHI.

## **12. Term and Termination**

This Agreement commences on the Effective Date and continues until the termination of the underlying services relationship or until all PHI has been returned, destroyed, or protections extended. Covered Entity may terminate this Agreement if it determines that Business Associate has violated a material term and has failed to cure within thirty (30) days after written notice, or if cure is not feasible, immediately. Upon termination, Section 11 applies.

### 13. Compliance with Law Changes

The Parties shall take such action as is necessary to amend this Agreement from time to time as necessary to comply with the requirements of the HIPAA Rules and any other applicable law.

### 14. Remedies

**Injunctive relief.** Each Party acknowledges that breach of this Agreement may cause irreparable harm. The non-breaching Party is entitled to seek immediate injunctive relief without bond or proof of actual damages. **Attorney's fees.** The prevailing Party recovers reasonable attorney's fees to the extent permitted by law.

**Cumulative remedies.** All remedies are cumulative and in addition to any remedies available under the HIPAA Rules.

### 15. Required Disclosures and Protected Activity

**General whistleblower protection.** Nothing in this Agreement prohibits the reporting of suspected violations of law to any government agency, including reports to HHS or the Office for Civil Rights.

### 16. Indemnification

Business Associate shall indemnify, defend, and hold harmless Covered Entity and its officers, directors, employees, and agents from any claims, damages, fines, penalties, costs, and attorney's fees arising out of or relating to any Breach of Unsecured PHI or violation of this Agreement by Business Associate or its Subcontractors.

### 17. General Provisions

**Governing Law.** State of [STATE], without prejudice to federal HIPAA requirements. **Venue.** Exclusive venue in [VENUE CITY FOR COURT OR ARBITRATION], [STATE].

**Assignment.** Business Associate may not assign without Covered Entity's prior written consent; Covered Entity may assign to successors.

**Severability; Waiver; Entire Agreement; Counterparts; Notices.** Ambiguities shall be resolved to permit compliance with the HIPAA Rules. Invalid provisions reformed to minimum extent. No waiver except in signed writing. This Agreement, together with any underlying services agreement, is the entire agreement on its subject matter; in the event of conflict, this Agreement controls as to PHI. Counterparts and electronic signatures permitted under ESIGN. Notices to preamble addresses.

## Signatures

### Covered Entity

\_\_\_\_\_  
PRINTED NAME

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
DATE

**Business Associate**

\_\_\_\_\_  
PRINTED NAME

\_\_\_\_\_  
SIGNATURE

\_\_\_\_\_  
DATE