

## Appendix K

### Business Associate Agreement

(Sample)

#### **I. Definitions:**

- a. "Business Associate" shall mean [CONTRACTOR].
- b. "Covered Program" shall mean [THE STATE], New York Department of Financial Services
- c. Other terms used, but not otherwise defined, in this AGREEMENT shall have the same meaning as those terms in the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") and implementing regulations, including those at 45 CFR Parts 160 and 164.

#### **II. Obligations and Activities of Business Associate:**

- a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law.
- b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
- c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
- d. Business Associate agrees to report to Covered Program any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware. Business Associate also agrees to report to Covered Program any Breach of Unsecured Protected Health Information of which it becomes aware. Such report shall include, to the extent possible:
  1. A brief description of the Breach, including the date of Breach and the date of discovery of the Breach, if known;
  2. A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security code, or other types of information were involved);
  3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
  4. A description of the Business Associate's investigation of the Breach, a plan to mitigate harm to individuals, and a plan to protect against any further Breaches; and

5. Contact procedures for Covered Program to inquire or learn additional information.

e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Program, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f. Business Associate agrees to provide access, at the request of Covered Program, and in the time and manner designated by Covered Program, to Protected Health Information in a Designated Record Set, to Covered Program or, as directed by Covered Program, to an Individual in order to meet the requirements under 45 CFR § 164.524.

g. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Program directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Program, in the time and manner designated by Covered Program.

h. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Program available to the Covered Program, or to the Secretary, in a time and manner designated by the Covered Program or designated by the Secretary, for purposes of the Secretary determining Covered Program's compliance with HIPAA, HITECH and 45 CFR § 164.528.

i. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Program to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

j. Business Associate agrees to provide to Covered Program, in time and manner designated by Covered Program, information collected in accordance with this Agreement, to permit Covered Program to comply with 45 CFR § 164.528.

k. Business Associate agrees to comply with the security standards for protection of electronic protected health information in 45 CFR § 164.308, 45 CFR § 164.310, 45 CFR § 164.312 and 45 CFR § 164.316.

### **III. Permitted Uses and Disclosure by Business Associate**

a. Except as otherwise limited in this AGREEMENT, Business Associate may only use or disclose Protected Health Information as necessary to perform functions, activities, or services for, or on behalf of, Covered Program as specified in this Agreement.

b. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

#### **IV. Term and Termination**

a. Term. The Term of this Agreement shall be effective as of [INSERT EFFECTIVE DATE], and shall terminate when all of the Protected Health Information provided by Covered Program to Business Associate, or created or received by Business Associate on behalf of Covered Program, is destroyed or returned to Covered Program, or, if 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.

b. Termination for Cause. Upon Covered Program's knowledge of a material breach by Business Associate, Covered Program may provide an opportunity for Business Associate to cure the breach and end the violation or may terminate this AGREEMENT if Business Associate does not cure the breach and end the violation within the time specified by Covered Program, or Covered Program may immediately terminate this AGREEMENT if Business Associate has breached a material term of this AGREEMENT and cure is not possible.

c. Effect of Termination.

1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Program, or created or received by Business Associate on behalf of Covered Program. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Program notification of the conditions that make return or destruction infeasible. Upon mutual agreement of Business Associate and Covered Program that return or destruction of Protected Health Information is infeasible, Business Associate 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 Business Associate maintains such Protected Health Information.

## **V. Violations**

a. Any violation of this AGREEMENT may cause irreparable harm to the Covered Program. Therefore, the Covered Program may seek any legal remedy, including an injunction or specific performance for such harm, without bond, security or necessity of demonstrating actual damages.

b. Business Associate shall indemnify and hold the Covered Program harmless against all claims and costs resulting from acts/omissions of Business Associate in connection with Business Associate's obligations under this AGREEMENT. Business Associate shall be fully liable for the actions of its agents, employees, partners or subcontractors and shall fully indemnify and hold harmless the Covered Program from suits, actions, damages and costs, of every name and description relating to breach, notification required by 45 CFR Part 164 Subpart D, or State Technology Law § 208, caused by any intentional act or negligence of Business Associate, its agents, employees, partners or subcontractors, without limitation, provided however, that Business Associate shall not indemnify for that portion of any claim, loss or damage arising hereunder due to the negligent act or failure to act of Covered Program.

## **VI. Miscellaneous**

a. Regulatory References. A reference in this AGREEMENT to a section in the Code of Federal Regulations means the section as in effect or as amended, and for which compliance is required.

b. Amendment. Business Associate and Covered Program agree to take such action as is necessary to amend this AGREEMENT from time to time as is necessary for Covered Program to comply with the requirements of HIPAA, HITECH, and 45 CFR Parts 160 and 164.

c. Survival. The respective rights and obligations of Business Associate under Section (IV)(c) of this AGREEMENT shall survive the termination of this AGREEMENT.

d. Interpretation. Any ambiguity in this AGREEMENT shall be resolved to permit Covered Program to comply with HIPAA, HITECH and 45 CFR Parts 160 and 164.

e. HIV/AIDS. If HIV/AIDS information is to be disclosed under this AGREEMENT, Business Associate acknowledges that it has been informed of the confidentiality requirements of Public Health Law Article 27-F.