APPENDIX C

NYS Department of Civil Service

Employee Health Service
HIPAA Business Associate Requirements
June 2013

This Appendix sets forth the HIPAA Business Associate requirements incumbent upon the Contractor in its provision of services to and on behalf of the Employee Health Service of the New York State Department of Civil Service (EHS), insofar as the Contractor creates, receives, maintains, transmits, or otherwise accesses, uses, or discloses individually identifiable health information on behalf of the EHS in the course of the Contractor's delivery of services under the Contract.

I. Definitions. For purposes of this Appendix to the LOA:

A. "Business Associate" shall mean the Contractor.

B. "Covered Program" shall mean the Department of Civil Service Employee Health Service (EHS).

C. Other terms used, but not otherwise defined, in this Appendix 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 LOA or as required by law.

B. Business Associate agrees to use the appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by the LOA and to comply with the security standards for the protection of electronic protected health information in 45 CFR Part 164, Subpart 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 inconsistent with or in violation of the requirements of the LOA.

C. Business Associate agrees to report to the DCS as soon as reasonably practicable any use or disclosure of the Protected Health Information not provided for by the LOA of which it becomes aware. Business Associate also agrees to report to the

DCS 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 what happened, including the date of the Breach and the date of the 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 number, date of birth, home address, account number, diagnosis, disability 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 what Business Associate is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and
5. Contact procedures for the DCS to ask questions or learn additional information.

D. Business Associate agrees, in accordance with 45 CFR § 164.502(e)(1)(ii), to ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such information.

E. Business Associate agrees to provide access, at the request of the DCS, and in the time and manner designated by the DCS, to Protected Health Information in a Designated Record Set, to the DCS in order for the DCS to comply with 45 CFR § 164.524.

F. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the DCS directs in order for the DCS to comply with 45 CFR § 164.526.

G. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for the DCS to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528; and Business Associate agrees to provide to the DCS, in time and manner designated by the DCS, information collected in accordance with the LOA, to permit the DCS to comply with 45 CFR § 164.528.

H. Business Associate agrees, to the extent the Business Associate is to carry out the DCS' obligation under 45 CFR Part 164, Subpart E, to comply with the requirements of 45 CFR Part 164, Subpart E that apply to the DCS in the performance of such obligation.

I. 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, the DCS available to the DCS, or to the Secretary of the federal Department of Health and Human Services, in a time and manner designated by the DCS or the Secretary, for purposes of the Secretary determining the DCS' compliance with HIPAA, HITECH and 45 CFR Parts 160 and 164.

III. Permitted Uses and Disclosures by Business Associate.

A. Except as otherwise limited in the LOA, Business Associate may only use or disclose Protected Health Information as necessary to perform functions, activities, or services for, or on behalf of, the DCS as specified in the LOA.

B. Business Associate may use Protected Health Information for the proper management and administration of Business Associate.

C. Business Associate may disclose Protected Health Information as required by law.

IV. Term and Termination.

A. This Appendix shall be effective for the term effective for the LOA, after which time all of the Protected Health Information provided by the DCS to Business Associate, or created or received by Business Associate on behalf of the DCS, shall be destroyed or returned to the DCS; provided that, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information in accordance with the terms in this Appendix.

B. Termination for Cause. Upon the DCS' knowledge of a material breach by Business Associate, the DCS may provide an opportunity for Business Associate to cure the breach and end the violation or may terminate the LOA if Business Associate does not cure the breach and end the violation within the time specified by the DCS. Alternatively, the DCS may immediately terminate the LOA if Business Associate has breached a material term of the LOA and cure is not possible.

C. Effect of Termination.

1. Except as provided in paragraph (c)(2) below, upon termination of the LOA, for any reason, Business Associate shall return or destroy all Protected Health Information received from the DCS, or created or received by Business Associate on behalf of the DCS. 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 returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to the DCS notification of

the conditions that make return or destruction infeasible. Upon mutual agreement of Business Associate and the DCS that return or destruction of Protected Health Information is infeasible, Business Associate shall extend indefinitely the protections of this Appendix to such Protected Health Information and shall 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 Appendix may cause irreparable harm to the DCS. Therefore, the DCS 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 DCS harmless against all claims and costs resulting from acts/omissions of Business Associate in connection with Business Associate's obligations under this Appendix. Business Associate shall be fully liable for the actions of its agents, employees, partners or subcontractors and shall fully indemnify and save harmless the DCS 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. However, 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 the DCS.

VI. Miscellaneous.

A. Regulatory References. A reference in this Appendix 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 the DCS agree to take such action as is necessary to amend this Appendix from time to time as is necessary for the DCS 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 (IV)(C) of this Appendix shall survive the termination of the LOA.

D. Interpretation. Any ambiguity in this Appendix shall be resolved in favor of a meaning that permits the DCS to comply with HIPAA, HITECH and 45 CFR Parts 160 and 164.

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