Article IX — HIPAA Privacy and Security Practices

Article IX — HIPAA Privacy and Security Practices

§ 20A-901 In General.

This Plan, the Administrator, and the Employer shall comply in all respects with the applicable requirements of HIPAA, including the administrative simplification provisions as set forth in 45 CFR Part 160 and Part 162, the provisions that govern the privacy of Protected Health Information as set forth in 45 CFR Part 160 and Part 164, Subparts A and E, the provisions that govern notification in the case of breach of unsecured Protected Health Information as set forth in 45 CFR Part 160 and Part 164, Subparts A and D, and the provisions that govern the security of Protected Health Information as set forth in 45 CFR Part 160 and Part 164, Subparts A and C. All of these provisions are incorporated into this Article by reference as if set forth in full. The HIPAA privacy and security official of the Employer is the Borough Manager.

§ 20A-902 Definitions.

For purposes of this Article IX, the terms defined in this Section shall have the meanings indicated herein, whether with or without initial capital letters, unless the context in which they are used clearly indicates a different meaning:

(a) Covered Individual. The term "Covered Individual" shall mean a Participant or Covered Family Member.

(b) Electronic Protected Health Information. The term "Electronic Protected Health Information" shall have the same meaning as described in 42 CFR § 160.103, and generally includes Protected Health Information that is transmitted by electronic media or maintained in

electronic media. Unless otherwise specifically noted, Electronic Protected Health Information shall not include enrollment/disenrollment information and Summary Health Information.

(c) HIPAA. The term "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations promulgated thereunder from time to time.

(d) Protected Health Information. The term "Protected Health Information" shall have the same meaning as described in 45 CFR § 160.103, and generally includes individually identifiable health information held by, or on behalf of, the Plan.

(e) Summary Health Information. The term "Summary Health Information" means information (1) that summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor ha provided health benefits under a health plan; and (2) from which the information described at 42 CFR § 164.514(b)(2)(i) has been deleted, except that the geographic information described in 42 CFR § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five-digit ZIP code.

(f) Other Terms. Other terms used in this Article which are not defined in this Chapter but which have a definite meaning under HIPAA shall have the same meaning as when used in HIPAA, unless the context in which they are used clearly indicates a different meaning.

§ 20A-903 Employer's Certification of Compliance.

The Employer hereby certifies to the Plan and the Administrator that the Plan document (this Chapter 20A) incorporates the provisions of 45 CFR § 164.504(f)(2)(ii), and the Employer hereby agrees to the conditions of disclosure set forth in this Article.

§ 20A-904 Permitted Disclosures to the Employer for Plan Administration Purposes.

(a) In General. Unless otherwise permitted by law, the Plan may disclose a Covered Individual's Protected Health Information to the Employer if the Employer will use or disclose such Protected Health Information only for Plan Administration Purposes.

(b) Plan Administration Purposes. For purposes of this Section, the term "Plan Administration Purposes" means administrative functions performed by the Employer on behalf of the Plan, such as making payment of claims as certified to the Employer by the Plan Administrator, payment of administrative fees, quality assurance, auditing, monitoring, and investigation of fraud, abuse, or unlawful acts related to the Plan, and reporting, disclosure, and other obligations that are required by law or specifically authorized by HIPAA or other applicable law, and contemplated by the notice of privacy practices distributed by the Plan in accordance with 45 CFR § 164.520. Plan Administrative Purposes do not include functions performed by the Employer in connection with any other benefit or benefit plan of the Employer, and they do not include any employment-related functions. Any disclosure to and use by the Employer of a Covered Individual's Protected Health Information will be subject to and consistent with the provisions of this Article (including but not limited to § 20A-905) and the specifications and

requirements of the applicable portions of the HIPAA implementing regulations at 45 CFR Parts 160 through 164.

§ 20A-905 Restrictions on the Employer's Use and Disclosure of Protected Health Information.

(a) Employer will neither use nor further disclose a Covered Individual's Protected Health Information, except as permitted or required by this Chapter or as required by law.

(b) Employer will ensure that any agent, including any subcontractor, to which it provides a Covered Individual's Protected Health Information received from the Plan, agrees to the same restrictions, conditions, and security measures of this Chapter that apply to Employer with respect to the Protected Health Information.

(c) Employer will not use or disclose a Covered Individual's Protected Health Information for employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of Employer.

(d) Employer will report to the Plan and the Plan Administrator any use or disclosure of a Covered Individual's Protected Health Information that is inconsistent with the uses and disclosures allowed under this Chapter of which the Employer becomes aware.

(e) Employer will make Protected Health Information available to the Plan and the Plan Administrator or to the Covered Individual who is the subject of the information in accordance with 45 CFR § 164.524.

(f) Employer will make a Covered Individual's Protected Health Information available for amendment, and will on notice amend a Covered Individual's Protected Health Information, in accordance with 45 CFR § 164.526.

(g) Employer will track disclosures it may make of a Covered Individual's Protected Health Information that are accountable under 45 CFR § 164.528 so that it can make available the information required for the Plan to provide an accounting of disclosures in accordance with 45 CFR § 164.528, and will make available such information.

(h) Employer will make its internal practices, books, and records relating to its use and disclosure of a Covered Individual's Protected Health Information received from the Plan available to the Plan, the Administrator, and the U.S. Department of Health and Human Services to determine compliance with the HIPAA Privacy Rule at 45 CFR Part 164, Subpart E.

(i) Employer will, if feasible, return or destroy all Protected Health Information of a Covered Individual, in whatever form or medium, received from the Plan, including all copies thereof and all data, compilations, or other works derived therefrom that allow identification of any Covered Individual who is the subject of the Protected Health Information, when the Covered Individual's Protected Health Information is no longer needed for the plan administration functions for which the disclosure was made. If it is not feasible to return or destroy all such Protected Health Information, Employer will limit the use or disclosure of any Covered Indivi-

dual's Protected Health Information that cannot feasibly be returned or destroyed to those purposes that make the return or destruction of the information infeasible.

(j) Employer will ensure that the adequate separation between the Plan and the Employer (*i.e.*, the "firewall") required in § 20A-907 and 45 CFR § 504(f)(2)(iii), is satisfied.

§ 20A-906 Other Disclosures to the Employer.

Nothing in this Article shall prohibit or in any way limit the Plan from disclosing a Covered Individual's Protected Health Information to the Employer where HIPAA permits such disclosure in the absence of the requirements of §§ 20A-904 and 20A-905, including, to the extent permitted by HIPAA, the disclosure of Protected Health Information:

(a) that is Summary Health Information, upon the request of the Employer for the purpose of modifying, amending, or terminating this Plan;

(b) on whether an individual is participating in the Plan; or

(c) pursuant to and in accordance with a valid individual authorization under the HIPAA Privacy Rule.

§ 20A-907 Adequate Separation Between the Employer and the Plan.

(a) Employees of the Employer to be Given Access to Information. Only the Borough Manager and the Borough Treasurer may be given access to a Covered Individual's Protected Health Information received by the Employer from the Plan or a business associate servicing the Plan, except that members of Borough Council may be given access to the information described in § 20A-906(a) or (b).

(b) Purposes of Use. The persons identified in subsection (a) will have access to a Covered Individual's Protected Health Information only to perform the plan administration functions specified in § 20A-904 that Employer provides for the Plan, or in accordance with permitted disclosures made under § 20A-906.

(c) Disciplinary Action. The persons identified in subsection (a) will be subject to disciplinary action and sanctions pursuant to the Employer's employee discipline and termination procedures, for any use or disclosure of a Covered Individual's Protected Health Information in breach of or violation of or noncompliance with the provisions of this Article. Such disciplinary action may include one or more of the following to the extent not inconsistent with other applicable disciplinary policies: written or oral warning or reprimand, required additional training and education, limitations on or revocation of access to Protected Health Information, diminution of duties, suspension, probation, disqualification for bonus or other pay or promotion, demotion in pay or status, referral for criminal prosecution, a requirement to reimburse the Plan or Employer for damages, removal from position, or discharge.

§ 20A-908 Investigation of Incidents of Noncompliance.

If the Employer becomes aware of any issues relating to noncompliance with the requirements of this Article, the Employer shall undertake an investigation to determine the extent, if any, of such noncompliance; the individuals, policies, practices, or procedures responsible for the noncompliance; and, to the extent feasible, appropriate means for curing or mitigating the effects of noncompliance and preventing such noncompliance in the future.

§ 20A-909 Security Measures for Electronic Protected Health Information.

The Borough Manager will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic Protected Health Information that the Employer creates, receives, maintains, or transmits on behalf of the Plan.

§ 20A-910 Notification of Security Incidents.

The Employer will report to the Plan and the Administrator any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations in the Employer's information systems, of which the Employer becomes aware.