

**NY44 HEALTH BENEFITS PLAN TRUST
GROUP HEALTH BENEFITS**

HIPAA PRIVACY POLICY

A. Introduction

NY44 Health Benefits Plan Trust (the “Trust”) sponsors the following self-funded group health benefits:

- Medical
- Prescription Drug Benefits
- Vision Benefits
- Dental Benefits

For purposes of this **HIPAA Privacy Policy (“Privacy Policy”)**, the self-funded benefits listed above are referred to collectively and singularly as the “Plan.”

Members of the Trust’s workforce may have access to protected health information (“PHI”) of Plan participants: (1) on behalf of the Plan itself; or (2) on behalf of the Trust, for administrative functions of the Plan and other purposes permitted by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) privacy rules. HIPAA and its implementing regulations restrict the Plan’s and the Trust’s ability to use and disclose protected health information.

Protected Health Information. PHI means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. PHI includes information of persons living or deceased, including genetic information.

This Privacy Policy will govern the circumstances under which, if any, Plan PHI may be shared with any such other plans.

It is the Trust’s policy that the Plan shall comply with HIPAA’s requirements for the privacy of PHI. To that end, all members of the Trust’s workforce who have access to PHI must comply with this Privacy Policy. For the purposes of this Privacy Policy, the Trust’s workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, Trustees and other persons whose work performance is under the direct control of the Trust, whether or not they are paid by the Trust. The term “employee” includes all of these types of workers.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Privacy Policy. The Trust reserves the right to amend or change this Policy at any time (and even retroactively)

without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Plan or the Trust. To the extent this Policy is in conflict with the HIPAA privacy rules, the HIPAA privacy rules shall govern.

B. Plan's Responsibilities as Covered Entity

I. Privacy Officer and Contact Person

Stacey Porter, the Trust's Benefits Specialist, is the Privacy Officer for the Plan. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy of the Plan's PHI, including but not limited to this Privacy Policy. The Privacy Officer will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

The Privacy Officer is responsible for ensuring that the Plan complies with the provisions of the HIPAA privacy rules regarding business associates, including the requirement that the Plan have a HIPAA-compliant Business Associate Agreement in place with all business associates, and that all business associates have written contractual agreements in place with any subcontractor or vendor with whom it shares PHI in accordance with 45 C.F.R. § 164.314. The Privacy Officer shall also be responsible for monitoring compliance by all business associates with the HIPAA privacy rules and this Privacy Policy.

II. Workforce Training

It is the Trust's policy to train all members of its workforce who have access to Plan PHI on the Plan's Policy and Procedures. The Privacy Officer is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their Plan functions in compliance with HIPAA.

III. Safeguards and Firewall

The Trust will establish on behalf of the Plan appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of PHI.

Technical safeguards include limiting access to information by creating computer firewalls.

Physical safeguards include locking doors or filing cabinets.

Firewalls will ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for plan administrative functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

IV. Privacy Notice

The Privacy Officer is responsible for developing and maintaining the Plan's Notice of Privacy Practices ("NOPP") that describes:

- the uses and disclosures of PHI that may be made by the Plan;
- the rights of individuals under HIPAA privacy rules;
- the Plan's legal duties with respect to the PHI; and
- other information as required by the HIPAA privacy rules.

The NOPP will inform participants that the Trust will have access to PHI in connection with its plan administrative functions. The NOPP will also provide a description of the Plan's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The NOPP shall be placed on the Plan's or the Trust's website. The notice also will be individually delivered:

- at the time of an individual's enrollment in the Plan;
- to a person requesting the notice; and
- to participants within 60 days after a material change to the notice.

The Plan will also provide notice of availability of the NOPP (or a copy of the NOPP) at least once every three years in compliance with the HIPAA privacy regulations.

Additionally, the Plan will prominently post any changes or revisions to the NOPP on its website by the effective date of the material change to the NOPP, or otherwise, provide information about the material change and how to obtain the revised NOPP, in its next annual mailing to individuals then covered by the Plan.

V. Complaints

Stacey Porter, the Plan's Privacy Officer, sporter@e1b.org, will be the Plan's contact person for receiving complaints.

The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of HIPAA or this Privacy Policy will be imposed in accordance with the Trust's discipline policy, up to and including termination.

VII. Mitigation of Inadvertent Disclosures of PHI

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of an individual's PHI in violation of HIPAA or the policies and procedures set forth in this Privacy Policy. As a result, if an employee or business associate becomes aware of an unauthorized use or disclosure of PHI, either by an employee or a business associate, the employee or business associate must immediately contact the Privacy Officer so that appropriate steps to mitigate harm to the participant can be taken.

VIII. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility under the Plan.

IX. Plan Document

The Plan Document shall include provisions to describe the permitted and required uses and disclosures of PHI by the Trust for plan administrative or other permitted purposes. Specifically, the Plan Document shall require the Trust to:

- not use or further disclose PHI other than as permitted by the Plan Document or as required by law;
- ensure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to the Trust through a written contractual agreement in accordance with 45 C.F.R. § 164.314;
- not use or disclose PHI for employment-related actions;
- not use or disclose genetic information for underwriting purposes;
- report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Plan participants, in paper and/or electronic form, consider their amendments and, upon request, provide them with an accounting of PHI disclosures in accordance with the HIPAA privacy rules;

- make the Trust’s internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services (“HHS”) upon request; and
- if feasible, return or destroy all PHI received from the Plan that the Trust still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. Trust will ensure that all business associates return or destroy all PHI received from Trust, and that all business associates’ subcontractors and vendors return or destroy PHI received from the business associate as well in accordance with the written contractual agreement referenced above.

The Plan Document must also require the Trust to: (1) certify to the Privacy Officer that the Plan Document has been amended to include the above restrictions and that the Trust agrees to those restrictions; and (2) provide adequate firewalls in compliance with the HIPAA privacy rules.

X. Documentation

The Plan’s privacy policies and procedures shall be documented and maintained for at least six (6) years from the date last in effect. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual’s privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six (6) years.

C. Policies on Use and Disclosure of PHI

I. Use and Disclosure Defined

The Plan will use and disclose PHI only as permitted under HIPAA. The terms “use” and “disclosure” are defined as follows:

Use. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Trust, or by a Business Associate (defined below) of the Plan.

Disclosure. For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the Trust, or not to a Business Associate (defined below) of the Plan.

II. Workforce Must Comply With Plan’s Policy and Procedures

All members of the Trust’s workforce (described at the beginning of this Policy and referred to herein as “employees”) who have access to Plan PHI must comply with this Policy.

III. Permitted Uses and Disclosures for Plan Administration Purposes

The Plan may disclose to the Trust for its use the following: (1) de-identified health information relating to plan participants; (2) Plan enrollment information; (3) summary health information for the purposes of obtaining premium bids for providing health insurance coverage under the Plan or for modifying, amending, or terminating the Plan; or (4) PHI pursuant to an authorization from the individual whose PHI is disclosed.

The Plan may disclose PHI to the following members of the workforce who have access to use and disclose PHI to perform functions on behalf of the Plan or to perform plan administrative functions (“employees with access”):

- Trust Staff; and
- Trustees.

Employees with access may disclose PHI to other employees with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Employees with access may not disclose PHI to employees (other than employees with access) unless an authorization is in place or the disclosure otherwise is in compliance with this Privacy Policy. Employees with access must take all appropriate steps to ensure that the PHI is not disclosed, available, or used for employment purposes. For purposes of this Policy, “plan administrative functions” include the payment and health care operation activities described in Section IV(C) of this Policy.

IV. Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the Plan’s own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan’s responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care.

Payment also includes:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk-adjusting based on enrollee status and demographic characteristics;
- billing, claims management, collection activities, obtaining payment under a contract for re-insurance (including stop-loss insurance and excess loss insurance) and related health care data processing; and
- any other payment activity permitted by the HIPAA privacy regulations.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

Health Care Operations. Health care operations means any of the following activities:

- conducting quality assessment and improvement activities;
- reviewing health plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development;
- business management and general administrative activities; and
- other health care operations permitted by the HIPAA privacy regulations.

V. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the Trust's "non-group health plan" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required or allowed by applicable state law and particular requirements under HIPAA are met.

VI. Mandatory Disclosures of PHI

A participant's PHI must be disclosed in the following situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows);
- The disclosure is required by law; or
- The disclosure is made to HHS for purposes of enforcing HIPAA.

VII. Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The requirements include prior approval of the Plan's Privacy Officer. Permitted are disclosures:

- about victims of abuse, neglect or domestic violence;
- for treatment purposes;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- for cadaveric organ-, eye- or tissue-donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

VIII. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures

made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

IX. Complying With the “Minimum-Necessary” Standard

To the extent practicable, the Plan’s will limit its use and/or disclosure of PHI to a Limited Data Set. A Limited Data Set is PHI that excludes the following identifiers of the individual or of relatives or household members of the individual:

- Names;
- Postal address information, other than town or city, State, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

If it is not practicable for the Plan to limit its use and/or disclosure of PHI to a Limited Data Set, the Plan will use the “minimum necessary” PHI to accomplish the purpose of the use or disclosure.

Minimum Necessary When Disclosing PHI. The Plan, when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. All disclosures not discussed in this Privacy Policy must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. The Plan, when requesting PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Plan is requested. All requests not discussed in this Policy must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

X. Disclosures of PHI to Business Associates

Employees may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate that it will appropriately safeguard the information through a business associate agreement in accordance with 45 C.F.R. § 164.314. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate contract is in place.

Business Associate is an entity that:

- performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI; or
- a subcontractor that creates, receives, maintains or transmits PHI on behalf of another business associate.

XI. Disclosures of De-Identified Information

The Plan may freely use and disclose information that has been "de-identified" in accordance with the HIPAA privacy regulations. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

XII. Prohibited Uses and Disclosures

The Plan will not use or disclose genetic information for underwriting purposes in accordance with 45 C.F.R. § 164.502.

XIV. Breach Notification Requirements

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers that there is a breach of Unsecured PHI and pursuant to the Policy and Procedure for Notification of a Breach of Unsecured Protected Health Information.

D. Policies on Individual Rights

I. Access to PHI and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Plan will provide paper and/or electronic access to PHI and it will consider requests for amendment that are submitted in writing by participants.

Designated Record Set is a group of records maintained by or for the Plan that includes:

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

The Plan will provide participants with the information requested in the electronic form and format requested by the participant and/or Trust if it is readily producible in such form and format; or, if not, in a readable electronic form and format as requested by the participant and/or Trust.

II. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, except for electronic disclosures of Electronic Health Records (“EHRs”), for which the right to an accounting extends to disclosures made in the last three years. The right to an accounting does not exist where the disclosure was:

- to carry out treatment, payment, or health care operations (except in the case of EHRs, for which this exception does not apply);

- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- part of a limited data set;
- for specific national security or law enforcement purposes; or
- made prior to the compliance date under HIPAA.

The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings.

III. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. The Plan will only honor reasonable requests and those requests that are required by law. The decision to honor such a request shall be made by the Privacy Officer.

However, the Plan shall accommodate such a request if the participant clearly states that the disclosure of all or part of the information could endanger the participant. The Privacy Officer has responsibility for administering requests for confidential communications.

IV. Requests for Restrictions on Use and Disclosure of PHI

A participant may request restrictions on the use and disclosure of the participant's PHI. The Plan may, but need not, honor such requests. The decision to honor such a request shall be made by the Privacy Officer. However, the Privacy Officer cannot deny such a request if the participant has paid for a service in-full, and the disclosure is not otherwise required by law.