NY44 Health Benefits Plan
HIPAA Security Policy

Introduction

The NY44 Health Benefits Plan is an employee welfare benefit plan sponsored by certain school districts and BOCES in New York State. They are referred to herein as "Employers" and "plan sponsors."

The Plan is administered by a governing board of trustees (the "Board") comprised of labor and management representatives of the employers.

The Plan is administered by a third-party administrator and has one or more business associates that perform functions for the Plan.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology For Economic and Clinical Health Act ("HITECH Act") and their implementing regulations and guidance require the Plan to implement various security measures with respect to electronic protected health information (electronic PHI).

Electronic Protected Health Information (EPHI) is protected health information that is transmitted by or maintained in electronic media.

Protected Health Information (PHI) is the information that is subject to and defined in the Plan's privacy policies and procedures. For purposes of this Policy, PHI does not include the following, referred to this Policy as "Exempt Information":

(1) summary health information, as defined by HIPAA's privacy rules, for purposes of (a) obtaining premium bids or (b) modifying, amending, or terminating the Plan;

(2) enrollment and disenrollment information concerning the Group Health Plan which does not include any substantial clinical information; or

(3) PHI disclosed to the Plan and/or Employers under a signed authorization that meets the requirements of the HIPAA privacy rules.

Electronic Media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

It is the Plan's policy to comply fully with the requirements of HIPAA's security regulations.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Plan reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent that 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. This Policy does not address requirements under state law or federal laws other than HIPAA.

I. Security Official

The Plan Administrator is the Security Official for the Plan. The Security Official is responsible for the development and implementation of the Plan's policies and procedures relating to security, including but not limited to this Policy.

II. Risk Analysis

The Plan’s Board of Directors will have access to PHI and EPHI only when administering the Plan’s claims procedure. The Board of Directors will have access to summary health information within the meaning of 45 CFR §164.504(a) to consider and price modifications to the Plan. Otherwise, all of the Plan's functions, including creation and maintenance of its records, are carried out by employees of the Employers and by business associates of the Plan. Further, the Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Employers, the third-party administrator and other business associates. Accordingly, the Employers and business associates create and maintain all of the electronic PHI relating to the Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Plan, and control their employees, agents, and subcontractors who have access to electronic PHI relating to the Plan. The Plan has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the Plan. That

ability lies solely with the Employers, the third-party administrator and other business associates.

Because the Plan has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Employers, the third-party administrator and other business associates affecting the security of Plan electronic PHI, and the Plan Sponsor, the third-party administrator and other business associates have undertaken certain obligations relating to the security of electronic PHI that they handle in relation to the performance of administrative functions for the Plan, the Plan's policies, and procedures, including this Policy, do not separately address the following standards (including the implementation specifications associated with them) established under HIPAA that are set out in Subpart C of 45 CFR Part 164:

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;
- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

The HIPAA security policies and procedures of the Employers and the third-party administrator and other business associates for electronic PHI of the Plan for the standards listed above are adopted by the Plan.

III. Risk Management

The Plan manages risks to its electronic PHI by limiting vulnerabilities, based on its risk analyses, to a reasonable and appropriate level, taking into account the following:

- The size, complexity, and capabilities of the Group Health Plan;
- The Plan’s technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and,
- The criticality of the electronic PHI potentially affected.

Based on risk analysis discussed in section II, the Plan made a reasoned, well-informed and good-faith determination on the implementation of the HIPAA security regulations

that it need not take any additional security measures, other than the measures set forth herein and the measures of the Employers, the third-party administrator, and other business associates, to reduce risks to the confidentiality, integrity and availability of electronic PHI.

IV. Group Health Plan Document

The Plan document shall include provisions requiring the Employers to:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the Employers create, receive, maintain, or transmit on behalf of the Plan (the Plan electronic PHI);

- ensure that reasonable and appropriate security measures support the Plan document provisions providing for adequate separation between the Plan and the Plan Sponsor (which were adopted as described in the Plan's privacy policy);

- ensure that any agents or subcontractors to whom the Employers provide Plan electronic PHI agree to implement reasonable and appropriate security measures to protect the Plan electronic PHI; and

- report to the Security Official any security incident of which the Employers become aware.

V. Disclosures of Electronic PHI to Third-Party Administrator and Other Business Associates

A business associate is an entity (other than the Employers), such as a third-party administrator, that:

- performs or assists in performing a Plan function or activity involving the use and disclosure of protected health information (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.

The Plan permits the third-party administrator and other business associates to create, receive, maintain, or transmit electronic PHI on its behalf. The Plan has obtained or will obtain satisfactory assurances from all business associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA security regulations and specifically providing that the business associate will:

- implement administrative, physical, and technical safeguards and documentation requirements that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the Plan (the Contract electronic PHI);

- ensure that any agents or subcontractors to whom the business associate provides Contract electronic PHI agree to implement reasonable and appropriate security measures to protect the Contract electronic PHI;

- report to the Group Health Plan any security incident of which the business associate becomes aware;

- take required steps with respect to breach notification requirements; and

- authorize termination of the contract by the Plan if the Plan determines that the business associate has violated a material term of the contract.

VI. 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 a breach of unsecured PHI.

VII. Documentation

The Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of Plan electronic PHI, and any changes to policies or procedures will be documented promptly.

Except to the extent that they are carried out by an Employer or business associates, the Plan shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented (including amendment of the Plan document in accordance with this policy, for example).

Policies, procedures, and other documentation controlled by the Plan may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The Plan will make its policies, procedures, and other documentation available to the Security Official and the Employers, the third-party administrator and other business associates or other persons responsible for implementing the procedures to which the documentation pertains.

The undersigned Secretary of the Board of Trustees of the NY44 Health Benefits Plan hereby certifies that the above Security Policy was approved by the Board of Trustees at a meeting held on the 5th day of November , 2013

_____

Secretary