NY44 Health Benefits Plan
HIPAA Privacy Policy

A. 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.

Certain members of an Employer'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 Employer, for administrative functions of the Plan and other purposes permitted by the HIPAA privacy rules.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Plan's and the Employers' ability to use and disclose protected health information.

> *Protected Health Information.* Protected health information 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. Protected health information includes information of persons living or deceased.

It is the Board's policy that the Plan shall comply with HIPAA's requirements for the privacy of PHI. To that end, all members of an Employer's workforce who have access to PHI must comply with this Privacy Policy. For purposes of this Policy and the Plan's more detailed Privacy Use and Disclosure Procedures, an Employer's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Employer, whether or not they are paid by the Employer. 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 Policy. The Board 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 Employers. This Policy does not address

requirements under other federal laws or under state laws. 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 Official and Contact Person

The Plan Administrator will be the Privacy Official for the Plan. The Privacy Official 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 and the Plan's Privacy Use and Disclosure Procedures. The Privacy Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI.

The Privacy Official 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. The Privacy Official 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 Board's policy to train all members of each Employer’s workforce who have access to Plan PHI on the Plan's Policy and privacy use and disclosure procedures. The Privacy Official 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

Each Employer will be required to establish the 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 Official is responsible for developing and maintaining a notice of the Plan's privacy practices 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 privacy notice will inform participants that their Employer will have access to PHI in connection with its plan administrative functions. The privacy notice 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 privacy notice 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.

V. Complaints

Dr. Darleen Michalak, 716-821-7074 will be the Plan's contact person for receiving complaints.

The Privacy Official 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. The complaint procedure is set forth in the privacy notice.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with each Employer’s discipline policy up to and including termination. All Employer employees with access to PHI of the Plan must sign the Confidentiality Agreement attached as an Appendix to this Policy.

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 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 Official 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 Employer for plan administrative or other permitted purposes. Specifically, the Plan document shall require the Employer to:

- not use or further disclose PHI other than as permitted by the Plan documents 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 Employer;
- not use or disclose PHI for employment-related actions;
- report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures in accordance with the HIPAA privacy rules;
- make the Employer'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 Employer 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.

The Plan document must also require the Employer to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the Employer 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 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 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 an Employer, 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 an Employer, or not to a Business Associate (defined below) of the Plan.

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

All members of an Employer'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 and with the Plan's Privacy Use and Disclosure Procedures, which are set forth in a separate document.

III. Permitted Uses and Disclosures for Plan Administration Purposes

The Plan may disclose to an Employer 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 persons or employees 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”):

- Board members
- Dr. Darleen Michalak, Plan Administrator
- Thomas Pomidoro, Claims Analyst
- Alice Riley, Fiscal Agent
- Jeni Kapalczynski, Assistant to the Plan Administrator

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 Policy and Plan's privacy use and disclosure procedures. 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 C.IV 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 Operation. Health care operation 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 an Employer's "non-health" 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 Plan's Privacy Use and Disclosure Procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Plan's Privacy Official. 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

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual;

- uses or disclosures made pursuant to a valid authorization;
- disclosures made to HHS;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

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 must be reviewed on an individual basis with the Privacy Official 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 must be reviewed on an individual basis with the Privacy Official 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. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Official 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.

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. Breach Notification Requirements

The Plan will comply with the Reportable Breach Notification Policy set forth in Appendix B of this Policy.

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 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.

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, other than disclosures:

- to carry out treatment, payment or health care operations 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;
- as part of a limited data set;
- for specific national security or law enforcement purposes; or
- disclosures that occurred prior to the compliance date.

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 Official 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 may, but need not, honor such requests. The decision to honor such a request shall be made by the Privacy Official.

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 Official 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 Official.

The undersigned Secretary of the Board of Trustees of the NY44 Health Benefits Plan Trust hereby certifies that the above amended Privacy Policy together with the attached Breach Notification Policy was approved by the Board of Trustees at a meeting held on the 5th day of November, 2013.

_____

Lori Sosenko
Secretary,
Board of Trustees

Appendix A to Privacy Policy: Employee Confidentiality Agreement

I, , have read and understand the Privacy Policy of the NY44 Health Benefits Plan, (the "Plan"), for the protection of the privacy of individually identifiable health information (or protected health information [PHI]), as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition, I acknowledge that I have received the Plan's policies concerning PHI use, disclosure, storage, and destruction as required by HIPAA.

In consideration of my employment or compensation by the Employer, I hereby agree that I will not at any time—either during my employment or association with the Employer or Plan or after my employment or association ends—use, access, or disclose PHI to any person or entity, internally or externally, except as is required and permitted in the course of my duties and responsibilities with the Employer, as set forth in the Plan's privacy policies and procedures or as permitted under HIPAA. I understand that this obligation extends to any PHI that I may acquire during the course of my employment or association with the Employer or the Plan, whether in oral, written or electronic form and regardless of the manner in which access was obtained.

I understand and acknowledge my responsibility to apply the Plan's policies and procedures during the course of my employment or association. I also understand that any unauthorized use or disclosure of PHI will result in disciplinary action, up to and including the termination of employment or association with the Employer and the imposition of civil penalties and criminal penalties under applicable federal and state law, as well as professional disciplinary action as appropriate.

I understand that this obligation will survive the termination of my employment or end of my association with the Employer, regardless of the reason for such termination.

Signed: _____ Date: _____

Print Name: _____

Appendix B to Privacy Policy: Reportable Breach Notification Policy

I. Introduction

This Reportable Breach Notification Policy is adopted by the Plan as part of the Plan's Privacy Policy and is intended to comply with the Interim Final Rule, Breach Notification for Unsecured Protected Health Information, issued by the Department of Health and Human Services (HHS) ("Breach Regulations"). It applies to breaches occurring on or after September 23, 2009.

Under the Breach Regulations, if a reportable breach of unsecured PHI has occurred, the Plan must comply with certain notice requirements with respect to the affected individuals, HHS, and, in certain instances, the media.

II. Identifying a Reportable Breach

The first step is to determine whether a Reportable Breach has occurred. If a Reportable Breach has not occurred, the notice requirements do not apply.

The Privacy Official is responsible for reviewing the circumstances of possible breaches brought to her attention and determining whether a Reportable Breach has occurred in accordance with this Reportable Breach Notification Policy and the Breach Regulations.

- All Business Associates, and all workforce members who have access to PHI, are required to report to the Privacy Official any incidents involving possible breaches.

There is a Reportable Breach only if all of the following have occurred, as determined by the Privacy Official:

- There is a violation of the HIPAA Privacy Rules involving "unsecured" PHI.
- The violation involved unauthorized access, use, acquisition, or disclosure of unsecured PHI.
- The violation resulted in a significant risk of harm to the individual(s) whose unsecured PHI was involved.
- No exception applies.

The Privacy Official's determination of whether a Reportable Breach has occurred will include the following considerations:

- *Was there a violation of HIPAA Privacy Rules?* There must be an impermissible use or disclosure resulting from or in connection with a violation of the HIPAA Privacy Rules by the Plan or a Business Associate of the Plan. If not, then the notice requirements do not apply.
- *Was PHI involved?* If not, then the notice requirements do not apply.
- *Was the PHI secured?* (For electronic PHI to be "secured," it must have been encrypted to NIST standards or destroyed. For paper PHI to be "secured," it must have been destroyed.) If yes, then the notice requirements do not apply.

- *Unauthorized access, use, acquisition, or disclosure of PHI.* The violation of HIPAA Privacy Rules must have involved one of these. If it did not, then the notice requirements do not apply.
- *Significant Risk of Harm.* The violation must have resulted in significant risk of harm to the individual. If it did not, then the notice requirements do not apply. The harm may be financial, reputational, or other harm.

To determine whether a risk of harm is significant, the Privacy Official will perform a risk assessment that considers various factors, which may include some or all of the following:

- *Who impermissibly used or to whom was the PHI impermissibly disclosed?* For example, if the disclosure was to another HIPAA covered entity or to a federal agency or other entity subject to privacy rules similar to HIPAA Privacy Rules, then there is probably not a significant risk of harm to the individual.
- *Was the PHI returned or destroyed prior to being accessed?* For example, if the Plan obtains satisfactory assurance or a binding agreement from the recipient that the PHI will be destroyed or not further used or disclosed, there is probably not a significant risk of harm to the individual. Similarly, if the PHI in question was returned prior to it being accessed for improper purpose (e.g., return of a computer that was not hacked into), there is probably not a significant risk of harm to the individual.
- *What type and amount of PHI was involved in the impermissible use or disclosure?* Generally, the greater the amount of PHI and the greater the risk that the individual can be identified by disclosed PHI, the more likely its disclosure creates a significant risk of harm.

If the Privacy Official determines that there was not a significant risk of harm to the affected individual(s), the Plan will document the determination in writing and keep the documentation on file.

If an exception applies, the notice requirements do not apply.

- *Exception 1:* The notice requirements do not apply if the breach involved an inadvertent unauthorized access, use, acquisition, or disclosure to an employee, volunteer, or other workforce member or Business Associate and no further unauthorized access, use, acquisition, or disclosure occurred, if—(a) the unauthorized access, use, acquisition or disclosure was in good faith; and (b) the unauthorized access, use, acquisition, or disclosure was within the scope of authority of a workforce member or Business Associate. (For example, the exception might apply to an inadvertent email to the wrong co-worker; but if an unauthorized employee looks up the PHI of his neighbor, the exception does not apply.)
- *Exception 2:* The notice requirements do not apply if the breach involved an inadvertent disclosure from one person authorized by the Plan to have access to PHI to another person authorized by the Plan to have access to PHI.
- *Exception 3:* The notice requirements do not apply if the breach involved a disclosure where there is a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI. (For

example, an EOB mailed to wrong person and returned to the Plan unopened, or a report containing PHI is handed to the wrong person, but is immediately pulled back before the person can read it.)

III. If a Reportable Breach Has Occurred: Notice Timing and Responsibilities

If the Privacy Official determines that a Reportable Breach has occurred, the Privacy Official will determine (in accordance with the Breach Regulations) the date the breach was discovered in order to determine the time periods for giving notice of the Reportable Breach. The Plan has reasonable systems and procedures in place to discover the existence of possible breaches, and workforce members are trained to notify the Privacy Official or other responsible person immediately so the Plan can act within the applicable time periods.

The Privacy Official is responsible for the content of notices and for the timely delivery of notices in accordance with the Breach Regulations. However, the Privacy Official may, on behalf of the Plan, engage a third party (including a Business Associate) to assist with preparation and delivery of individual notices.

The Breach Regulations may require a breach to be treated as discovered on a date that is earlier than the date the Plan had actual knowledge of the breach. The Privacy Official will determine the date of discovery as the earlier of—(a) the date that a workforce member (other than a workforce member who committed the breach) knows of the events giving rise to the breach; and (b) the date that a workforce member or agent of the Plan, such as a Business Associate (other than the person who committed the breach) would have known of the events giving rise to the breach by exercising reasonable diligence.

Except as otherwise specified in the notice sections that follow, notices must be given "without unreasonable delay" and in no event later than 60 calendar days after the discovery date of the breach. Accordingly, the investigation of a possible breach, to determine whether it is a Reportable Breach and the individuals who are affected, must be undertaken in a timely manner that does not impede the notice deadline.

There is an exception to the timing requirements if a law enforcement official asks the Plan to delay giving notices.

IV. Business Associates

If a Business Associate commits or identifies a possible Reportable Breach relating to Plan participants, the Business Associate must give notice to the Plan. The Plan is responsible for giving notices of the Reportable Breach.

Unless otherwise required under the Breach Regulations, the discovery date for purposes of the Plan's notice obligations is the date that the Plan receives notice from the Business Associate.

In its Business Associate contracts, the Plan will require Business Associates to—

- report incidents involving breaches or possible breaches to the Privacy Official in a timely manner;
- provide to the Plan any and all information requested by the Plan regarding the a breach or possible breach, including, but not limited to, the information required to be included in notices (as described below); and
- establish and maintain procedures and policies to comply with the Breach Regulations, including workforce training.

V. Notice to Individuals

Notice to the affected individual(s) is always required in the event of a Reportable Breach. Notice will be given without unreasonable delay and in no event later than 60 calendar days after the date of discovery (as determined above).

1. Content of Notice to Individuals

Notices to individuals will be written in plain language and contain all of the following, in accordance with the Breach Regulations:

- A brief description of the incident.
- If known, the date of the Reportable Breach and the Discovery Date.
- A description of the PHI involved in the Reportable Breach (for example, full name, SSN, address, diagnosis, date of birth, account number, disability code, or other).
- The steps individuals should take to protect themselves (such as contacting credit card companies and credit monitoring services.
- A description of what the Plan is doing to investigate the Reportable Breach, such as filing a police report or reviewing security logs or tapes.
- A description of what the Plan is doing to mitigate harm to individuals.
- A description of what measures the Plan is taking to protect against further breaches (such as sanctions imposed on workforce members involved in the Reportable Breach, encryption, and installation of new firewalls).
- Contact information for individuals to learn more about the Reportable Breach or ask other questions, which must include at least one of the following: Toll-free phone number, email address, website, or postal address.

2. Types of Notice to Individuals

The Plan will deliver individual notices using the following methods, depending on the circumstances of the breach and the Plan's contact information for affected individuals. *Actual Notice* will be given in all cases, unless the Plan has insufficient or out-of-date addresses for the affected individuals. Actual notice—

- will be sent via first-class mail to last known address of the individual(s);
- may be sent via email instead, if the individual has agreed to receive electronic notices;
- will be sent to the parent on behalf of a minor child; and

- will be sent to the next-of-kin or personal representative of deceased person.

Substitute Notice will be given if the Plan has insufficient or out-of-date addresses for the affected individuals.

- If addresses of fewer than ten living affected individuals are insufficient or out-of-date, substitute notice may be given by telephone, in person, or via email.
- If addresses of ten or more living affected individuals are insufficient or out-of-date, substitute notice must be given via either website or media.

— *Substitute notice via website.* Conspicuous posting on home page of the website of the Plan or Employer for 90 days, including a toll-free number to obtain information about the Reportable Breach. Contents of the notice can be provided directly on website or via hyperlink.

— *Substitute notice via media.* Conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, including a toll-free number to obtain information about the Reportable Breach. It may be necessary to give the substitute notice in both local media outlet(s) and statewide media outlet(s).

- Substitute Notice is required only for living persons.

Urgent Notice will be given, in addition to other required notice, in circumstances where imminent misuse of unsecured PHI may occur. Urgent notice must be given by telephone or other appropriate means.

- Example: Urgent notice is given to an individual by telephone. The Plan must also send an individual notice via first-class mail.

VI. Notice to HHS

Notice of all Reportable Breaches will be given to HHS. The time and manner of the notice depends on the number of individuals affected. The Privacy Official is responsible for both types of notice to HHS.

Immediate Notice to HHS. If the Reportable Breach involves 500 or more affected individuals, regardless of where the individuals reside, notice will be given to HHS without unreasonable delay, and in no event later than 60 calendar days after the date of discovery (as determined above). Notice will be given in the manner directed on the HHS website.

Annual Report to HHS. The Privacy Official will maintain a log of Reportable Breaches that involve fewer than 500 affected individuals, and will submit a report of to HHS every year by the last day in February (60 calendar days after January 1) of the Reportable Breaches that occurred in the preceding calendar year. The reports will be submitted as directed on the HHS website.

VII. Notice to Media (Press Release)

Notice to media (generally in the form of a press release) will be given if a Reportable Breach affects more than 500 individuals who are residents of any one State or jurisdiction. For example:

- If a Reportable Breach affects 600 individuals who are residents of New York, notice to media is required.
- If a Reportable Breach affects 450 individuals who are residents of New York and 60 individuals who are residents of Pennsylvania, notice to media is not required.

If notice to media is required, notice will be given to prominent media outlets serving the State or jurisdiction. For example:

- If a Reportable Breach involves residents of one city, the prominent media outlet would be the city's newspaper or TV station.
- If a Reportable Breach involves residents of various parts of the state, the prominent media outlet would be a statewide newspaper or TV station.

If notice to media is required, it will be given without unreasonable delay, and in no event more than 60 calendar days after the date of discovery (as determined above). The content requirements for a notice to media are the same as the requirements for a notice to individuals. The Privacy Official is responsible for giving notice to media.