

Employee Health Plans of TOWN OF HAMPSTEAD

HIPAA Privacy Policies and Procedures

Draft 04/13/2010

Employee Health Plans of TOWN OF HAMPSTEAD

HIPAA Privacy Policies and Procedures

TABLE OF CONTENTS

EFFECTIVE DATE.....	1
DEFINITIONS.....	1
USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION.....	4
No Use or Disclosure of Genetic Information for Underwriting Purposes	5
Minimum Necessary Standard.....	6
SECURITY AND CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION	7
PLAN PRIVACY OFFICIAL.....	7
BREACH NOTIFICATION	7
COMPLAINT POLICY	8
PLAN DOCUMENTS\INSURANCE CONTRACTS POLICY	10
PARTICIPANT RIGHTS	10
Requests for Amendment of Protected Health Information	10
Requests for Access to PHI	12
Requests for Restrictions on Uses and Disclosures	14
Requests for Confidential Communications	14
Requests for Accounting of Certain Disclosures	15
SANCTIONS AND MITIGATION	16
RECORDKEEPING	17
SECURITY STANDARDS	18
TRAINING	18
PRIVACY NOTICE	18
ELECTRONIC TRANSACTIONS	19
BUSINESS ASSOCIATE AGREEMENTS	19
Exhibit A.....	21

Employee Health Plans of TOWN OF HAMPSTEAD

HIPAA PRIVACY POLICIES AND PROCEDURES

This document describes the policies and procedures that TOWN OF HAMPSTEAD, as Plan Administrator for its employee health plans, has adopted to provide for the integrity, security, privacy and availability of health information that is maintained by or on behalf of those plans. The policies and procedures described in this document are intended to comply with all requirements of the HIPAA Privacy Regulations as they apply to those health plans and will be construed to be consistent with those requirements, where reasonable, and will be modified to match those requirements, as needed. This document also is intended to help provide for the Plan's compliance with all applicable HIPAA Privacy requirements of Subtitle D of the "Health Information Technology for Economic and Clinical Health Act" (the "HITECH Act") and any authoritative guidance issued pursuant to that Act, if and as they become applicable to the Plan.

If there is any conflict between the requirements of the Privacy Regulations or Subpart D of the HITECH Act and any provision of this document, applicable law will control. Also, any amendment or revision or authoritative guidance relating to the Privacy and Security Regulations or of Subpart D of the HITECH Act is hereby incorporated into this document as of the date that the Plan is required to comply with that guidance.

This document uses the phrase, "the Plan", to refer to each of the separate employee health plans or benefit options sponsored by TOWN OF HAMPSTEAD[, or its affiliates (collectively referred to as "TOWN OF HAMPSTEAD" in this document)], including any plans or benefit options that provide coverage or reimbursement for medical, dental, vision, prescription drug or long term care expenses including any health care flexible spending arrangements and including any employees of TOWN OF HAMPSTEAD who are responsible for handling health information maintained by those health plans as well as any service providers who handle health information under contract with those health plans. This document is intended to apply to each of those benefit plans or options separately and collectively.

With respect to any fully insured health plan or benefit option offered by TOWN OF HAMPSTEAD, the insurance issuer generally is responsible for compliance with the requirements of the Regulations. Nothing in this document should be taken as requiring TOWN OF HAMPSTEAD to perform any function or compliance obligation that is imposed on an insurer and not on TOWN OF HAMPSTEAD as Plan sponsor. For fully insured coverage, this document is intended to provide for the Plan's compliance with the Regulations only to the extent that TOWN OF HAMPSTEAD, or a service provider (other than the insurer) that contracts with the Plan or with TOWN OF HAMPSTEAD, is actually involved in the use or disclosure of PHI on behalf of the Plan.

EFFECTIVE DATE

This document is effective 04/13/2010, except as otherwise provided below.

DEFINITIONS

Administrative Simplification Regulations or "Regulations" refers to regulations issued by the Department of Health and Human Services ("DHHS") pursuant to the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, and includes but is

not limited to the *Privacy Regulations* (the regulations issued as “Standards for Privacy of Individually Identifiable Health Information”); the *Electronic Transactions Standards* (the regulations issued as the “Standards for Electronic Transactions”); the *Security Standards* (the regulations issued as the “Security Standards”) and the *National Provider Identifier Standards* (the regulations issued as the “Standard Unique Identifier for Health Care Providers” Final Rule). In applying any references in this document to any of Regulations, the Plan will refer to the Regulations as modified and as in effect at the time the reference is to be applied. The Regulations will be interpreted in light of any guidance from DHHS or any other federal agency that the Plan determines is authoritative. To the extent that compliance with a regulatory provision or other guidance is not required, the Plan has discretion to follow or to decline to follow that provision.

Business Associate is defined at Section 160.103 of the Privacy Regulations and refers to a person or organization, other than TOWN OF HAMPSTEAD or its employees, that, pursuant to an agreement with TOWN OF HAMPSTEAD or the Plan, performs services on behalf of the Plan that require the use or disclosure of PHI by the Business Associate.

Covered Entity is defined at Section 160.103 of the Privacy Regulations and means an entity that is subject to the requirements of the Privacy Regulations, including, except as otherwise provided in the Privacy Regulations, health plans and health care clearinghouses plus any health care provider that transmits health information electronically in connection with a transaction that is subject to the Electronic Transaction Standards.

Designated Record Set is defined at Section 164.501 of the Privacy Regulations means a set of records (including paper and electronic records) maintained by or for the Plan that include PHI and that are either (1) enrollment, claims processing or medical management records or (2) any other records used by the Plan to make decisions about individuals. This term is used to refer to the set of records associated with an individual to which the individual has a right of access.

Health Care Operations means any of the following activities (as described in more detail in the Privacy Regulations) of the Plan (or another covered entity) to the extent that the activities relate to the Plan’s (or the other covered entity’s) administration:

- Conducting quality assessment and improvement activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- Enrollment, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care;
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- Business planning and development; and
- Business management and general administrative activities of the entity.

Limited Data Set means PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- Names;
- Postal address information, other than town or city, State and zip code;
- Telephone numbers;
- Fax numbers;
- E-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.

Payment means activities undertaken by the Plan (or by another covered entity, to the extent that those activities relate to the Plan) to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits or to obtain or provide reimbursement for health care. Payment activities include, but are not limited to: determining eligibility or coverage, adjudicating or subrogating of health benefit claims, risk adjusting, billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing; reviewing health care services to determine medical necessity, coverage, appropriateness of care, or justification of charges; utilization review activities, including precertification and preauthorization of services, and concurrent and retrospective review of services; and disclosure to consumer reporting agencies of certain protected health information relating to the collection of premiums or reimbursement.

Personal Representative means a person legally authorized, as determined under applicable State law, to act on behalf of another person, either generally or for a specified purpose, with respect to that other person. If, at any time, there is a substantial question as to whether a person who purports to be acting on behalf of any individual is authorized to do so, the Plan will require proof acceptable to the Plan that the purported personal representative is acting within the scope of his or her authority as a Personal Representative. However, except to the extent that the Plan has specific information to the contrary or that it appears unreasonable under the circumstances, the Plan ordinarily will assume that a parent of a minor child is an authorized personal representative of that child. Any reference in these Policies and Procedures to a right or a responsibility of an individual who is the subject of any Protected Health Information possessed by the Plan should be understood as referring also to an authorized Personal Representative acting on behalf of that individual.

Protected Health Information (“PHI”) is individually identifiable health information. Health information is any **information maintained or received by the Plan** that relates to an individual’s health condition, health care or payment for health care. Health information is individually identifiable if there is a reasonable possibility that the identity of the individual can be determined from the information. Specifically, health information is individually identifiable if it includes the

individual's name, address or Social Security Number, or any other details from which his or her identity might be determined under the context in which it has been released.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Except as otherwise indicated in this document, any word or phrase used in this document that is defined in the Regulations should be understood as having the same meaning as applies under the Regulations.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

The Plan acknowledges that PHI normally is to be used or disclosed by the Plan only to the minimum extent necessary to operate the Plan. The "Minimum Necessary Standard" and its exceptions are described in more detail below.

The Plan's agents and representatives ordinarily will use or disclose PHI only for purposes of payment, treatment or health care operations. However, PHI may also be used or disclosed for certain other purposes, but only as described in this document.

If PHI is to be used or disclosed for any purpose that is not otherwise permitted under this document, an individual authorization for that use or disclosure will be obtained, in advance, from any individual whose information is to be used. If the Plan receives PHI subject to an individual authorization provided by the individual, the Plan will use or disclose PHI only as permitted under the authorization.

In addition, the Plan will disclose PHI only as permitted under the Regulations or applicable Federal or State law. Specifically, the Plan may disclose PHI as follows:

- To an individual, or a Personal Representative of an individual, who requests PHI relating to that individual. The Plan, in its discretion, may limit the release of information to an individual to the extent that the disclosure is not required by the Regulations. For example, psychotherapy notes, information compiled in anticipation of litigation and information provided for certain research purposes, may be withheld, if the Plan determines it is not required (or is not permitted) to disclose the information.
- To any person or organization, as required for purposes of payment, treatment or health care operations. The Minimum Necessary Standard applies, except if PHI is being released to a provider for treatment purposes. In that case, the entire medical record may be released. However, psychotherapy notes will not be disclosed without individual authorization. PHI will be disclosed to any person or organization (for payment, treatment or health care operations purposes) only if the person or organization receiving the information is subject to the Regulations and to the terms of any applicable authorization or other restriction, either directly or through a Business Associate contract.
- To DHHS, if permitted under the Regulations, to enable DHHS to verify that the Plan is complying with applicable Regulations.

- To appropriate State authorities, to the extent that the Secretary of Health and Human Services has determined that the disclosure is necessary:
 - to prevent fraud and abuse relating to health care or payment for health care;
 - for purposes of State regulation of insurance or health plans, as authorized under applicable law;
 - for State reporting on health care delivery or costs; or
 - to serve a compelling public health, safety or welfare need, if the Secretary has determined that the intrusion into privacy is warranted when balanced against the compelling need for the disclosure.
- For law enforcement purposes, to the extent required under the Regulations or applicable State law.

No Use or Disclosure of Genetic Information for Underwriting Purposes

Regardless of any other provision of this document, the Plan will not use or disclose PHI that is genetic information for underwriting purposes. For purposes of this rule, "genetic information" and "underwriting purposes" have the meanings that apply to those terms under the proposed amendments to the Privacy Regulations issued by DHHS in June of 2009 (as summarized below), but those definitions will be automatically modified in accordance with any subsequent guidance that replaces, amends or supplements those definitions.

Genetic Information, for any individual, means information about

- his or her genetic tests or the genetic tests of family members;
- the manifestation of a disease or disorder in family members; or
- any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member.

Genetic Information for any individual also includes the genetic information for a fetus carried by the individual or a family member or for any embryo legally held by the individual or family member utilizing an assisted reproductive technology.

Genetic Information does not include information about the sex or age of any individual.

Genetic Services means:

- A genetic test (i.e, an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes, but not including an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition);
- Genetic counseling (including obtaining, interpreting, or assessing genetic information); or
- Genetic education.

Underwriting Purposes means:

- Rules for, or the determination of, eligibility (including enrollment and continued eligibility)

for, or the determination of, benefits under the Plan (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

- The computation of premium or contribution amounts under the Plan (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
- The application of any preexisting condition exclusion under the Plan; and
- Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

Underwriting Purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the Plan.

Minimum Necessary Standard

If the Minimum Necessary Standard applies, the Plan will make reasonable efforts to limit the use or disclosure of PHI to the minimum amount necessary to accomplish the intended purpose. In addition, when requesting information from a Covered Entity or a Business Associate, the Plan will make reasonable efforts to limit the amount of PHI requested to the minimum amount necessary for the intended use or disclosure.

In applying the Minimum Necessary Standard, the Plan will comply with any regulations or other authoritative guidance issued pursuant to Section 13405(b) of the HITECH Act, beginning no later than the date that guidance becomes applicable to the Plan. Until that time, the Plan will treat the Minimum Necessary Standard as limiting information subject to that standard to the Limited Data Set, to the extent practicable, or, if needed by the Plan, to the minimum PHI necessary to accomplish the intended purpose of the use, disclosure or request.

The Plan, or a Business Associate acting on behalf of the Plan will make the decision of whether the disclosure meets the requirements of the Minimum Necessary Standard, in any case in which that standard applies.

The Minimum Necessary Standard applies to most routine uses and disclosures of PHI (such as for payment and health care operations purposes). However, it does not apply to:

- disclosures to providers for treatment purposes;
- uses and disclosures that are **required** for purposes of complying with the Regulations or with applicable law;
- uses or disclosures that are required to be made to DHHS; or
- disclosures to the individual who is the subject of the PHI or to a third party pursuant to a request **initiated** by the individual.

For routine recurring uses and disclosures, the Plan may develop consistent written policies and procedures for complying with the Minimum Necessary Standard, and those policies are incorporated into this document by this reference.

For non-routine uses and disclosures that are subject to the Minimum Necessary Standard, the determination of the minimum necessary amount will be made on an individual basis.

SECURITY AND CONFIDENTIALITY OF PROTECTED HEALTH INFORMATION

The Plan periodically assesses potential risks and vulnerabilities regarding PHI in its possession to develop and revise its policies and procedures for safeguarding protected information from loss or unauthorized use or disclosure.

The Plan has adopted the following procedures to limit access to PHI to only those persons who must have access to that information to perform Plan functions:

- THE TOWN OF HAMPSTEAD does not maintain paper and electronic files containing PHI other than enrollment information.
- Paper files are kept in secure locations, e.g., in offices, desks or filing cabinets that are locked when authorized personnel are not present.
- Care is taken to minimize incidental disclosure of PHI to unauthorized employees, clients or service providers. TOWN OF HAMPSTEAD does not receive or transmit PHI.
- Routine audits are conducted by the Plan Privacy Official to monitor access to protected information, including access, log-ins, updates and edits.
- Supervisors and other employees who are likely to receive PHI from a plan participant (e.g., an employee who is requesting help with a claim) are trained to politely refer the participant to an appropriate authorized and trained person. All employees who request help with claims are referred to the broker.
- Inactive files that contain PHI are stored or archived in secure locations, e.g., locked closets that are not accessible to unauthorized personnel or contractors.
- Paper copies of records containing PHI that are no longer needed are returned to the entity that provided the records or are shredded or burned or disposed of in some other way that reduces the risk of improper disclosure.

PLAN PRIVACY OFFICIAL

Until further notice, Tammy Palmer is designated by the Plan as the Plan Privacy Official. The Privacy Official will coordinate the implementation and management of the Plan's privacy policies and will regularly monitor the Plan's compliance with the relevant requirements of the Privacy Regulations.

BREACH NOTIFICATION

Following the discovery of any **Breach of Unsecured PHI**, TOWN OF HAMPSTEAD will notify any affected individuals without unreasonable delay and no later than 60 days after the discovery.

Breaches of Unsecured PHI also will be reported to DHHS in accordance with applicable

guidance from DHHS (details are available on the HHS Web site at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule>). For Breaches affecting fewer than 500 individuals, the Plan will maintain documentation of the Breach and report it to DHHS no later than 60 days after the end of the calendar year in which the Breach occurs. For any Breach affecting 500 or more individual, a report will be filed with DHHS by the same

For purposes of this Breach Notification Policy, **Breach** has the same meaning that applies under Interim Regulations issued by DHHS pursuant to the HITECH Act on August 24, 2009, as modified by any later regulations or other authoritative guidance and currently means the acquisition, access, use, or disclosure of and individual's PHI in a manner not permitted under the Privacy Regulations which poses a significant risk of financial, reputational, or other harm to the individual.

The following are excluded from the definition of **Breach**:

- Any use or disclosure of PHI that would qualify as a "limited data set", as defined in the Definitions Section of this document and that does not include a date of birth or zip code information.
- Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the Plan or a business associate, if made in good faith and within the scope of authority that does not result in further use or disclosure in a manner that would violate the Privacy Regulations.
- Any inadvertent disclosure by a person who is authorized to access PHI for the Plan to another person authorized to access PHI for the Plan, if the information received as a result of such disclosure is not further used or disclosed in a manner that would violate the Privacy Regulations.
- Any disclosure of PHI where the Plan or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by DHHS in guidance issued pursuant to the HITECH Act (details are available on the HHS Web site at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule>). Currently, the only method of making PHI unsecured is to make it encrypted in accordance with standards set by DHHS. All PHI that is not in electronic form is considered unsecured PHI.

COMPLAINT POLICY

The Plan has developed the following procedures for individuals to file complaints concerning the Plan's privacy policies and procedures or about any perceived violation of the individual's privacy rights.

No individual will be intimidated or retaliated against for filing a complaint. Employees who violate this policy are subject to disciplinary action, up to and including termination.

Until further notice, Tammy Palmer, will be responsible for receiving and investigating Plan Privacy Policy complaints submitted to the Plan.

Complaints must be filed in writing with the Plan's designated complaint contact person (or office). However, a complaint is deemed to be submitted in writing to the Plan if a designated complaint contact person agrees to accept a complaint provided in person or over the telephone and documents the complaint on a Complaint Report Form. A complaint is received by the Plan on the date the written complaint (or Complaint Report Form completed by a designated contact person) is submitted to (or completed by) a designated complaint contact person.

A designated complaint contact person will investigate each properly filed complaint. The Plan (i.e., a TOWN OF HAMPSTEAD employee who is responsible for handling health information on behalf of the Plan) and any other appropriate TOWN OF HAMPSTEAD representatives will make all reasonable efforts to cooperate and to facilitate the investigation.

A written response will be provided to the individual within sixty days from the date the complaint was filed.

A written summary of the complaint and action taken will be filed with the Plan Privacy Official. This summary and other complaint documents will be retained for at least six years.

Translators, interpreters, and readers who meet the communication needs of the individual may be provided during the complaint process.

An individual may designate a representative of his or her choice to represent the individual's interests during the complaint process.

Complaints that raise potential liability issues will be referred to the appropriate TOWN OF HAMPSTEAD employee or officer responsible for risk management.

All complaints received and all complaint dispositions will be documented and the documentation will be retained for at least six years.

At the option of any individual who has a complaint, a complaint may also be filed with the Department of Health and Human Services, Office of Civil Rights. The Plan will cooperate with any investigation of such a complaint.

Upon request, the Plan will provide the following contact information for filing a complaint with DHHS (if the complaint arises in Maryland, Delaware, the District of Columbia, Pennsylvania or Virginia):

Office for Civil Rights
U.S. Department of Health & Human Services
150 S. Independence Mall West - Suite 372
Philadelphia, PA 19106-9111
(215) 861-4441; (215) 861-4440 (TDD) (215) 861-4431 FAX

Contact information for other regions is available online at:

PLAN DOCUMENTS\INSURANCE CONTRACTS POLICY

The Plan's agents and representatives will ensure that the governing Plan documents, and, where applicable, the insurance contracts under which Plan benefits are provided include provisions required by the Regulations. The Plan's agents and representatives will provide PHI to the appropriate TOWN OF HAMPSTEAD representatives only if and to the extent that the Regulations and the governing Plan documents permit the disclosure.

PARTICIPANT RIGHTS

The Plan will comply with the requirements of the Privacy Regulations that create rights that individual participants (or their Personal Representatives) may exercise with respect to PHI maintained or created by or on behalf of the Plan.

The Plan has developed the following policies and procedures for complying with those participant right requirements:

Requests for Amendment of Protected Health Information

If an individual believes that PHI maintained by the Plan in a Designated Record Set is inaccurate or incomplete, he or she may request an amendment or correction of that information.

A request for an amendment or correction of PHI must be made in writing to the Plan's Privacy Official, must specify the PHI to be amended and must state a reason for the request.

The Plan may deny a request for amendment, if the Plan determines that the PHI or record that is the subject of the request:

- was not created by the Plan (unless the individual provides information to the Plan explaining why the originator of the PHI is no longer available to act on the requested amendment);
- is not part of the individual's health record;
- would not be available for inspection under federal law; or
- is accurate and complete.

The Plan will respond to a request for an amendment within sixty days after it receives the individual's request. In certain cases, the Plan may take up to an additional thirty days to respond to the request. In those cases, the Plan will provide a written statement of the reasons for the delay and the date by which the Plan expects to complete its action on the request.

If the Plan grants the individual's request for amendment, in whole or in part, the Plan will:

- amend the PHI or record that is the subject of the request for amendment;
- inform the individual that the amendment is accepted and ask the individual to identify the

relevant persons with whom the amendment should be shared and agree to have the Plan notify those persons; and

- within a reasonable time after receiving the individual's permission to notify the relevant parties, the Plan will provide the amended information to persons identified by the individual, and persons, including Business Associates, that the Plan knows have the PHI that is the subject of the amendment and that may have relied, or foreseeably could rely, on such information to the detriment of the individual.

If the Plan denies a requested amendment, in whole or in part, the Plan will provide a timely, written denial in plain language that includes:

- a description of the basis for the denial;
- a description of the individual's right to submit a written statement disagreeing with the denial and the procedure for filing such a statement;
- a statement that, if the individual does not submit a statement of disagreement, the individual may request that the Plan provide the individual's request for amendment and the denial with any future disclosure of the PHI that is the subject of the amendment; and
- a description of the Plan's complaint procedures. The description will include the name, or title, and telephone number of the contact person or office responsible for receiving complaints.

The Plan will permit the individual to submit a written statement disagreeing with the denial of all or part of the requested amendment and the basis of such disagreement. The Plan may reasonably limit the length of the statement.

The Plan may prepare a written rebuttal to the individual's statement of disagreement. If a rebuttal is prepared, the Plan will provide a copy to the individual who submitted the statement of disagreement.

The Plan will identify the record or PHI that is the subject of a disputed amendment and link the individual's request for an amendment, the Plan's denial of the request, the individual's statement of disagreement, if any, and the Plan's rebuttal, if any.

If the individual has not submitted a written statement of disagreement, the Plan must include the individual's request for amendment and its denial, or an accurate summary of that information, with any subsequent disclosure of the relevant PHI only if the individual has asked the Plan to do that.

When a subsequent disclosure is made using a "standard transaction" (an electronic transaction that is subject to the Electronic Transaction Standards) that does not permit the additional material to be included, the Plan must separately transmit the material required to the recipient of the standard transaction.

If the Plan is informed by another covered entity of an amendment to an individual's PHI the Plan will amend the PHI as provided in that amendment.

Requests for Access to PHI

If the Plan possesses PHI about an individual, the individual may request access to or copies of any information included in a Designated Record Set, with the following exceptions:

- The Plan is not required to provide access to PHI that consists of psychotherapy notes.
- The Plan is not required to provide access to PHI that consists of information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.
- The Plan is not permitted to provide access to PHI that is subject to the Clinical Laboratory Improvements Amendments of 1988, if access by the individual would be prohibited by law.
- The Plan is not required to provide access to PHI that is exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR Section 493.3(a)(2)).

Requests for access to PHI should be submitted in writing to the Plan's Privacy Official or to another designated person who has been trained with regard to the Plan's Privacy Policies and Procedures.

The Plan normally will respond to a request for access to PHI within 30 days after it receives the request. If the Plan approves the request, it will permit the access requested within that 30-day period. However, if the requested information is not maintained onsite by TOWN OF HAMPSTEAD, the Plan will respond to a request and permit access (if the request is approved) within 60 days from the date the request is received. If the Plan cannot respond to a request within the applicable 30-day or 60-day period, it may have one 30-day extension of time to reply, if it informs the individual, within the original time period, of the delay, including the reasons for the delay.

The Plan will permit access to records containing PHI at reasonable hours in specified locations. At the request of an individual, the Plan, in its discretion, may provide access in other locations. PHI will be provided in the form or format requested, if it is readily producible in that form or format. Otherwise, the information will be provided in a readable hard copy or in any other form acceptable to the individual.

The Plan will provide copies of specified information within a Designated Record Set, but reserves the right to charge reasonable fees to cover the costs of making such copies. Instead of providing certain PHI requested, the Plan may provide a summary of that information, if the individual agrees to accept such a summary. Also, the Plan may provide an explanation of PHI to which access is provided, if the individual agrees to accept such an explanation. The Plan may charge a reasonable fee to cover the cost of preparing a summary or an explanation. The Plan will comply with reasonable requests to provide copies or summaries or explanations by mail or by other delivery methods, as specified by the individual, but reserves the right to charge the individual for postage or other delivery charges. The individual will be informed of the amount of any fees before they are incurred.

If a request for access is denied in whole or in part, the following procedures will apply:

- The Plan will provide a written explanation of the reasons for the denial. The explanation

will also include (1) a description of the individual's right to request review of the denial (if the denial is reviewable, as described below) and (2) a description of the individual's right to file a complaint with the Secretary of Health and Human Services or with the Plan's complaint contact person (including the name or title and phone number of the contact person).

- If the denial applies only to a portion of the PHI requested, the plan will provide access to any other requested PHI.
- If the Plan does not possess the PHI requested by the individual, but knows where the information is maintained, the Plan will inform the individual where to direct a request for that information.

A denial of access is **not reviewable** if the denial is made for one of the following reasons:

- The requested PHI is not subject to the right of access (i.e., the PHI is subject to one of the exceptions listed at the beginning of this section).
- The requested PHI was created by or obtained by a health care provider in the course of research and the individual has agreed to a restriction of access (that is currently in effect at the time of the request).
- The requested PHI is subject to the Privacy Act and the denial of access meets the requirements of that Act.
- The requested PHI was obtained from someone (other than a health care provider) under a promise of confidentiality and release would likely reveal the source of the information.

An individual's request for access may also be denied for any of the following reasons, but the **denial will be reviewable**:

- A licensed health care professional has reviewed the requested PHI and has determined, in the exercise of professional judgment, that the requested access is reasonably likely to endanger the life or physical safety of the individual or another person.
- The requested PHI mentions another person (other than a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that providing access is reasonably likely to cause substantial harm to that other person.
- The request is made by a Personal Representative and a licensed health care professional has determined, in the exercise of professional judgment, that providing access to the Personal Representative is reasonably likely to cause substantial harm to the individual or another person.

If an individual requests a review of a denial of access (and the denial is reviewable), the Plan will promptly refer the request to a designated reviewing official, who will be a licensed health care professional who did not participate in the original denial. The reviewing official will make a decision on whether to deny or provide access within a reasonable period of time. The Plan will

deny or provide access according to the instructions of the reviewing official and will provide a notice of the reviewing official's determination to the individual.

Requests for Restrictions on Uses and Disclosures

A participant may request restrictions on uses and disclosures that may be made of PHI relating to that participant. This includes the uses and disclosures described above for treatment, payment and other health plan operations purposes.

However, under the law, the Plan is not required to accept any restriction (except as otherwise provided below).

The Plan will comply with reasonable requests for restrictions. However, if the Plan determines, in its discretion, that a requested restriction will interfere with the efficient administration of the Plan or is otherwise unacceptable, it may decline the request.

In one situation, the Plan is required to and will agree to a request for a restriction on disclosure of PHI if the disclosure would otherwise be made to another health plan for purposes of payment or health care operations. If the PHI to be disclosed is limited to a health care item or service for which the health care provider involved has been paid in full out-of-pocket by the individual (or by someone else, other than the Plan or other health coverage, on behalf of the individual, the Plan will agree to a request that such information not be provided to another health plan.

If the Plan agrees to a restriction, it will document the restriction and will abide by the terms of that restriction. The Plan will take reasonable steps to communicate any granted restriction to employees or Business Associates who should be aware of the restriction.

Requests for restrictions on uses and disclosures of PHI should be directed to the Plan's Privacy Official or to another person who has been trained with regard to the Plan's Privacy Policies and Procedures. The request should be in writing and should specify the records to which the restriction would apply and the limits of the requested restriction.

A restriction will terminate under the following conditions:

- The individual agrees to the termination in writing;
- The individual agrees to the termination verbally and the agreement is documented in writing; or
- Except for the type of restriction where the Plan is required to agree to the restriction, if the Plan informs the individual that it is terminating its agreement to the restriction, in which case, the restriction will not apply to any new information to which it would otherwise apply but will continue to apply to the information to which it applied before the Plan informed the individual of the termination.

Requests for Confidential Communications

If information that includes PHI is to be provided to an individual or to someone else on behalf of that individual, under certain circumstances, the individual has a right to request that the information be provided in an alternative, more confidential manner.

Under the Privacy Regulations, this right is guaranteed only if the individual clearly informs the Plan that the ordinary disclosure of part or all of the information might endanger the individual. For example, an individual may not want information about certain types of treatment to be sent to his or her home address because someone else who lives there might have access to it and might become abusive as a result of learning about the treatment. In such a case, the individual could request that the information be sent to an alternate address. The Plan will honor such a request as long as it is reasonable, but the Plan reserves the right to reject a request that it determines would impose too much of an administrative burden or financial risk on the Plan.

The Plan may require that a request for confidential communications be in writing and may require that the request include a statement that the release of some or all of the information to which the request pertains may endanger the individual. Beyond that requirement, the Plan will not require details about the purported danger.

In addition, the Plan, in its sole discretion, may agree to a request for confidential communication even if the individual does not indicate that ordinary disclosure will endanger the individual. As always, the Plan reserves the right to reject a request that it determines would impose an administrative burden or financial risk on the Plan.

Requests for confidential communications should be directed to the Plan's Privacy Official or to another person who has been trained with regard to the Plan's Privacy Policies and Procedures. The request should be in writing and should specify the records to which the request would apply and the limits of the request.

Requests for Accounting of Certain Disclosures

An individual may request an accounting of certain types of non-routine disclosures of PHI pertaining to that individual.

The following types of disclosures are **not** subject to the accounting requirement:

- disclosures that are made for **treatment, payment and health care operations** purposes;
- disclosures that are incidental to a use or disclosure otherwise permitted under the Privacy Regulations (for example, isolated cases where a legitimate conversation about PHI is overheard by an unauthorized person despite reasonable procedures in place to minimize such incidental disclosures);
- disclosures made pursuant to an individual authorization from the participant (or a Personal Representative);
- disclosures made to the participant (or a Personal Representative);
- disclosures to a person involved in the individual's care or for certain other purposes, as permitted under Section 164.510 of the Privacy Regulations;
- certain disclosures for national security or intelligence purposes, as provided in Section 164.512(k)(2) of the Privacy Regulations;

- certain disclosures to correctional institutions or law enforcement officials, as provided in Section 164.512(k)(5) of the Privacy Regulations; and
- disclosures as part of a “limited data set”, as permitted under Section 164.514(e) of the Privacy Regulations.

The Plan will keep appropriate records of any disclosures that are made that are subject to the accounting requirement.

A request for an accounting may not apply to any disclosures made before April 14, 2004 or for any period earlier than six years from the date the request is properly submitted to the Plan.

An individual may receive an accounting of disclosures once every 12 months at no charge. The Plan may charge a reasonable fee for any additional requests during a 12 month period.

Requests for an accounting of disclosures should be directed to the Plan’s Privacy Official or to another designated person who has been trained with regard to the Plan’s Privacy Policies and Procedures. The request should be in writing and should specify the period to which the request applies.

The Plan normally will respond to a request for an accounting within 60 days after it receives the request. However, if the Plan cannot respond to a request within the 60-day period, it may have one 30-day extension of time to reply, if it informs the individual, within the original time period, of the delay, including the reasons for the delay.

An accounting for disclosures will be provided in writing and a copy will be maintained by the Plan for at least six years from the date it is provided to the individual.

Although it is not anticipated that the Plan will maintain any PHI in the form of an Electronic Health Record (as that term is defined for purposes of Section 13405(c) of the HITECH Act), if and to the extent that the Plan does in fact maintain an Electronic Health Record for any individual, the Plan will comply with all applicable regulations and other authoritative guidance relating to accounting for disclosures of such records, beginning on the date that such regulations or other guidance becomes applicable to the Plan.

SANCTIONS AND MITIGATION

The Plan’s agents and representatives will work with the appropriate TOWN OF HAMPSTEAD representatives to investigate potential violations of the Regulations or of these Policies and Procedures. The Plan’s agents and representatives will, to the extent practicable, work with the appropriate TOWN OF HAMPSTEAD representatives and, if appropriate, with any affected Business Associates to mitigate the harmful effects of any violation of which the Plan is aware.

After any investigation or discovery of a violation, if an employee or other agent of TOWN OF HAMPSTEAD is determined to be responsible, in whole or in part, for a violation of the Regulations or these Policies and Procedures, the Plan Privacy Official (or another person designated to act on behalf of the Plan) will work with the Plan Sponsor to see that appropriate remedial or disciplinary action is taken, based on the severity of the violation and the culpability of the employee or other

agent. The Plan Privacy Official (or his or her designee) generally will recommend sanctions based on the following general guidelines:

- If the Plan Privacy Official (or his or her designee) determines that the individual's involvement in the violation resulted from a misunderstanding of the relevant policies, procedures or Regulations or was otherwise unintentional, the individual generally should receive additional training regarding the Plan's privacy procedures or will be reassigned to other duties, if appropriate.
- If the Plan Privacy Official (or his or her designee) determines that the individual's involvement in the violation reflects recklessness or intentional disregard of relevant policies, procedures or Regulations, additional training or reassignment may be required. In addition, more severe sanctions will be recommended, if appropriate based on the severity of the violation, including the potential harm that could be expected to result. In appropriate circumstances, these sanctions could include a suspension or termination of employment.
- If the Plan Privacy Official (or his or her designee) determines that a criminal violation has occurred or that a violation should be reported to any Federal or State agency, the Plan Privacy Official will report the violation as appropriate and the Plan will cooperate with any investigation.

Notwithstanding the above guidelines, TOWN OF HAMPSTEAD will bear the final responsibility for determining the appropriate sanction, if any, and reserves the right to impose any sanction (or none) that it determines, in its absolute discretion, is appropriate. Any disciplinary action will be subject to TOWN OF HAMPSTEAD's general employment policies, including the requirements of any applicable collective bargaining agreement.

RECORDKEEPING

The Plan will maintain health information privacy records and documents required to be maintained by the Plan pursuant to Section 164.530(j) of the Privacy Regulations. Records to be kept include:

- a copy of this "Policies and Procedures" document and any subsequent document which is intended to satisfy the policies and procedures standard of Section 164.530(i) of the Privacy Regulations;
- a copy of any document used by the Plan as a "Notice of Health Information Privacy Practices" to be provided to participants;
- a copy of any communication that is required under the Privacy Regulations to be in writing; and
- documentation of any action, activity or designation that is required under the Privacy Regulations to be documented.

Such records will be kept for at least six years after the date the record is created. For documents such as this "Policies and Procedures" document or any "Notice of Health Information Privacy Practices" provided to Plan participants, a copy of the document will be kept for at least six years after the last date on which the document is in effect. Records may be maintained in electronic or

paper form.

SECURITY STANDARDS

The Plan will maintain appropriate administrative, technical and physical safeguards to protect the privacy of PHI. To the extent that PHI is created, received, maintained or transmitted in an electronic format, the Plan will comply with all applicable requirements of the Security Standards.

TRAINING

The Plan's agents and representatives and the appropriate TOWN OF HAMPSTEAD representatives will see that each TOWN OF HAMPSTEAD employee who requires access to PHI relating to the Plan receives appropriate training regarding the relevant requirements of the Regulations and of these Policies and Procedures. The Plan will provide additional training to all such employees, as needed, following any relevant change to the Plan's policies and procedures. Each employee's compliance with the requirements of the regulation will be periodically monitored and employees will receive additional training if appropriate.

The Plan will maintain a list, attached to these procedures as Exhibit A, of those employees of the Plan Sponsor who have received training regarding the Plan's Privacy Policies and Procedures and the relevant requirements of the Privacy Regulations. Only those employees listed on Exhibit A will have access to PHI on behalf of the Plan. Exhibit A will be updated as needed. The policy described in this paragraph should not be interpreted as prohibiting access and use of PHI by business associates of the Plan (and their employees or agents), as permitted under a valid business associate agreement with the Plan.

The Plan will maintain (for at least six years) appropriate records regarding each employee's completion of training requirements.

PRIVACY NOTICE

The Plan will maintain a "Notice of Health Information Privacy Practices" ("Privacy Notice") that describes the Plan's health information privacy practices for Plan participants. The Plan will comply with the requirements specified in the Plan's Privacy Notice, which is incorporated into these Policies and Procedures by this reference. The Privacy Notice is intended to be and, where reasonable, is to be construed to be consistent with the Policies and Procedures described in the body of this document. To the extent that there is any conflict between the requirements specified in the Privacy Notice and in any other part of these Policies and Procedures, the Privacy Notice, as interpreted by the Plan Administrator and to the extent that the Privacy Notice is consistent with the requirements of the Regulations, will prevail.

The Regulations require that the Privacy Notice be distributed as follows:

- On or before the date the HIPAA Privacy Regulations become applicable to the Plan, to all employees who participate in any non-insured health plan option offered under the Plan, as of that date;
- Upon enrollment, to any employee who enrolls in any non-insured health plan option offered under the Plan, after the initial distribution of the Notice; and

- Within 60 days of any material revision to the Notice; to all employees who participate in any non-insured health plan option offered under the Plan.

In addition, at least once every three years, the Plan will inform current employees who participate in the Plan that the Notice is available and that a participant may obtain a copy of the Notice by requesting one from the Plan's Privacy Official (or some other specified person or office). This information may be included in the Plan's summary plan description or another document provided to participants as long as that approach satisfies the requirements mentioned in the previous sentence.

Whenever a new privacy notice is prepared, anyone who is receiving continuation coverage (pursuant to COBRA or any similar applicable State law), with respect to any non-insured health plan option under the Plan (a "continuee") at that time should receive a copy of the Notice, unless his or her coverage is dependent coverage provided because of another continuee's election of family continuation coverage. For anyone who becomes a continuee after the Notice is initially distributed, there is no need to provide a Notice merely because of the election of continuation coverage, because those individuals should have previously received a current Notice as an employee (or as a dependent of an employee who received the Notice on the dependent's behalf).

Except as described above, the Privacy Regulations does not require the Plan to automatically distribute a privacy notice to non-employee participants. However, the Plan's Privacy Notice will be available upon request to anyone covered under the Plan.

The Plan will initially distribute paper copies of the Privacy Notice, but it reserves the right to choose to distribute some or all future Privacy Notices by email as long as the specific requirements of Section 164.520(c)(3) of the Privacy Regulations (or any alternative subsequent regulatory requirements) are met. In addition, any website (on the Internet or on an internal Intranet) that provides information about employee benefits to employees will prominently display the Privacy Notice or a link to it and will make the Privacy Notice available for downloading. However, a paper copy of the Notice will always be available upon request to any participant.

Notwithstanding the above, the Privacy Regulations does not require the Plan to automatically distribute a Privacy Notice to participants in any fully-insured health plan or coverage option covered by these Policies and Procedures. Instead, the insurance issuer is required to provide a notice for such participants. However, the Plan's Privacy Notice will be available upon request to participants in any insured health plan covered by these Policies and Procedures.

ELECTRONIC TRANSACTIONS

The Plan, together with its Business Associates, where appropriate, will comply with all applicable requirements of the Electronic Transactions Standards when engaging in a covered transaction. In addition, the Plan's contracts with any Business Associate will include provisions requiring the Business Associate to conduct any covered transaction engaged in on behalf of the Plan according to the applicable standards.

BUSINESS ASSOCIATE AGREEMENTS

For purposes of any non-insured health plan options offered under the Plan, any Business Associate of the Plan will be required, as a condition for receiving, creating, disclosing or maintaining PHI for the Plan, to comply with the requirements of the Administrative Simplification Regulations, as they

apply to the Plan. For such Business Associates, the Plan will enter into a written agreement (or an amendment to another agreement) that meets the Business Associate agreement requirements of the Regulations, as they apply to the Plan.

With respect to any insured health plan option available under the Plan, the obligation to obtain a business associate agreement generally applies to the insurer rather than to TOWN OF HAMPSTEAD as a Plan sponsor.

Exhibit A

The following persons have been designated by the Plan Sponsor as authorized to use or disclose Protected Health Information for purposes of the Plan and have received appropriate training regarding the Plan's Health Information Privacy Policies and Procedures and the applicable requirements of the Privacy Regulations. Any person on this list is authorized to access PHI on behalf of the Plan beginning on the date training has been completed and ending on the date that he or she is no longer authorized to access PHI (e.g., because of termination of employment or a change in responsibilities).

Name	Date training completed	Date no longer authorized to access PHI
Tammy Palmer	03/17/2010	