HIPAA POLICY AND PROCEDURE MANUAL
For Town of West Boylston Massachusetts

Effective as of

November 18, 2015

TABLE OF CONTENTS

POLICY OVERVIEW AND HANDLING PROTECTED HEALTH INFORMATION

Overview of Policies and Procedures to Protect the Privacy of Protected Health Information

Policy

The policies and procedures set forth in this manual (referred to collectively as the HIPAA Policy) are intended to protect the privacy of Protected Health Information in accordance with amendments to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; and updates to the HIPAA Rules, , as set forth in the Department of Health and Human Services regulations at 45 CFR Parts 160 and 164 et seq.

This HIPAA Policy shall apply to any and all Protected Health Information maintained, used or disclosed with respect to certain group health plans and emergency medical services maintained by Town of West Boylston, Massachusetts (collectively referred to as the "Plan") as set forth in the Appendix to this HIPAA Policy and emergency medical services provided by the West Boylston Fire department.

Except as otherwise provided for in the HIPAA Policy and in the respective plan documents or permitted under the Final Rule set forth at 45 CFR Parts 160 and 164 et seq. only employees who are designated as HIPAA Authorized Employees shall have access to Protected Health Information maintained by the Plan. The members of HIPAA Authorized Employees shall be:

- The Privacy Contact appointed pursuant to Section 1.3 of this HIPAA Policy; and
- The positions listed in the Appendix to this HIPAA Policy.

For purposes of this HIPAA Policy, members covered by 45 CFR Parts 160 and 164 et seq. shall, unless otherwise noted, be treated as acting on behalf of the Plan.

HIPAA Authorized Employees shall maintain, use or disclose Protected Health Information in accordance with the procedures set forth in the Appendix, provided doing so does not result in a violation of this HIPAA Policy or HIPAA's Privacy or Security Rules. No member of HIPAA Authorized Employees shall use or disclose Protected Health Information for employment related actions or decisions nor shall such

member use or disclose such information in connection with any other benefit or employee benefit plan of the Town.

Key terms are defined in the Glossary at Section 4 of this HIPAA Policy.

Minimum Necessary Policy

Policy

HIPAA Authorized Employees shall ensure that the Protected Health Information used and disclosed under the HIPAA Policy is, to the extent required under the HIPAA Privacy Rule, only the minimum necessary to accomplish the purpose of the use or disclosure.

Requests for Protected Health Information shall be processed pursuant to this HIPAA Policy or 45 CFR Parts 160 and 164 et seq.

An employee's entire medical record may not be used or disclosed unless the release has been authorized pursuant to a HIPAA Authorization or it has been specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.

The methods of, and conditions for, access, storage or destruction of Protected Health Information in paper form, electronic form or any other form shall be periodically evaluated by the Town's Privacy Contact to ensure the applicable requirements under this HIPAA Policy and 45 CFR Parts 160 and 164 et seq.

Procedure

1. Any requests for the use and/or disclosure of Protected Health Information shall be forwarded to and handled by members of HIPAA Authorized Employees pursuant to this HIPAA Policy. Unless otherwise provided in this HIPAA Policy, only members of HIPAA Authorized Employees shall have access to all Protected Health Information used, disclosed or maintained by the Plan.

2. In the event of a request for use or disclosure of an employee's entire medical record, such record may not be used or disclosed except when production of the record has been specifically authorized by the employee in writing or is otherwise required by law.

3. In the case of routine uses and disclosures or Protected Health Information, and unless as required under this HIPAA Policy, HIPAA Authorized Employees may make the use or disclosure which he or she reasonably believes is the minimum necessary to accomplish the purpose of the use or disclosure. Any non-routine use or disclosure of Protected Health Information shall be reviewed by the Privacy Contact prior to the use or disclosure of the Protected Health Information.

4. This minimum necessary policy shall not apply to:

    - Disclosures to or requests by a health care provider for treatment;

- Uses or disclosures made to the individual who is the subject of the Protected Health Information;
- Uses or disclosures made pursuant to a written authorization;
- Disclosures made to the Secretary of the Department of Health and Human Services;
- Uses or disclosures that are required by law; and
- Uses or disclosures that are required for compliance with applicable requirements of the HIPAA Privacy Rule.

The Privacy Contact shall periodically monitor and review the methods of and conditions for access to and storage of Protected Health Information in paper form, electronic form or any other form to ensure the applicable requirements under this HIPAA Policy and 45 CFR Parts 160 and 164 et seq. are satisfied.

Appointment and Duties of the Privacy Contact

Policy

West Boylston, Massachusetts shall appoint a Privacy Contact (and set forth such appointment in the Appendix to this HIPAA Policy) to implement and oversee compliance with the requirements of the HIPAA Privacy Rule.

The Privacy Contact is responsible for developing and implementing, in coordination with 45 CFR Parts 160 and 164 et seq. as applicable to the Town of West Boylston, developing employee training programs, publishing and distributing notice of privacy practices and, except as otherwise provided in this HIPAA Policy, serving as the designated decision maker for issues and questions involving interpretation of HIPAA in conjunction with legal counsel. The Privacy Contact may appoint a HIPAA Authorized Employees to the HIPAA Policy Group. The HIPAA Policy group will at the direction and supervision of the Privacy Contact assist in the execution of the tasks assigned below. The Privacy Contact is responsible for the following tasks:

- Inventorying the uses and disclosures of all Protected Health Information as defined in the HIPAA Privacy Rule;
- Working with legal counsel and management, key departments and committees to ensure the Town of West Boylston has and maintains appropriate privacy consent and authorization forms and information notices and materials, including amendments to plan documents, negotiating Business Associate contracts and developing authorizations;
- Coordinating with employer functions such as FMLA leave, drug testing and (other physicals or testing required by the covered entity)
- Establishing and implementing appropriate firewalls and encryption technology between the Town of West Boylston, Massachusetts organization and its group health plans or third-party billing entities;
- Establishing procedures to ensure individual rights guaranteed by the HIPAA Privacy Rule are met;
- Setting up a complaint process and enforcement;
- Developing overall privacy policies and procedures for the covered plans;
- Establishing programs to audit and monitor Business Associates and internal privacy compliance where the Privacy Contact has been apprised that someone in the Town of West Boylston's employ and/or a Business Associate has failed to comply with45 CFR Parts 160 and 164 et seq. pursuant to HIPAA's privacy and security requirements and/or a Business Associate agreement;

- Keeping up to date on the latest privacy and security developments and federal and state laws and regulations that may affect the requirements under this HIPAA Policy;
- Reviewing all system-related information throughout the networks of the members of the Town of West Boylston to ensure alignment between security and privacy practices and to act as a liaison to the Town's information systems departments;
- Cooperation with the HHS Office of Civil Rights, other legal entities and the Town of West Boylston's officers in any compliance reviews or investigations; and
- Addressing questions from individuals concerning privacy practices and procedures.

Business Associate Agreements

Policy

The Plan shall enter into an agreement with each entity or person who is a Business Associate, as defined by HIPAA. Following the execution of a Business Associate Agreement, HIPAA Authorized Employees may disclose necessary Protected Health Information to a Business Associate and may allow that Business Associate to create or receive Protected Health Information **if, and only if**, the Town and the Business Associate have entered into a Business Associate agreement as described in this HIPAA Policy. The Town is not required to enter into a Business Associate agreement with a health care provider prior to disclosing information to such health care provider relating to the treatment of an individual.

Business Associate agreements shall include satisfactory assurances from each Business Associate, respectively, that it shall make reasonable efforts to ensure that all uses and discloses Protected Health Information shall be made only in accordance with the terms and conditions of the Business Associate Agreement, or as otherwise required under 45 CFR Parts 160 and 164 et seq. and that applicable HIPAA Breach Notification requirements are met.

The original copy of the Business Associate agreement, executed by all parties, shall be maintained pursuant to the Record Retention and Documentation Policy.

Prior to disclosing any Protected Health Information to a Business Associate, HIPAA Authorized Employees shall confirm that a current Business Associate agreement is on file. If no Business Associate agreement is on file, HIPAA Authorized Employees may not disclose any Protected Health Information to the Business Associate until such an agreement is on file. If HIPAA Authorized Employees is unable to obtain an executed Business Associate agreement from the Business Associate, HIPAA Authorized Employees may not disclose any Protected Health Information to the Business Associate.

To the extent that the Town has actual knowledge of a violation of any Business Associate agreement or HIPAA's Privacy or Security Rules, the Town shall take reasonable steps to ensure that breach notification requirements are met.

Uses and Disclosures of Protected Health Information Authorization is Required/Not Required

Policy

Subject to the exceptions described below, the Plan shall not use or disclose Protected Health Information unless it first obtains a valid written authorization from the individual to whom the Protected Health Information relates, in the form provided in the Appendix to this HIPAA Policy. When the Plan receives a valid authorization, the use and disclosure of the Protected Health Information shall be made according to the terms of the authorization.

Exceptions to Authorization Requirement. The members of HIPAA Authorized Employees may use or disclose Protected Health Information without first obtaining an authorization and without providing the employee with the opportunity to agree or object under the following circumstances:

- disclosure to the individual about whom the Protected Health Information relates;
- use or disclosure made to facilitate Treatment, Payment or Health Care Operations;
- use or disclosure incident to (that is, as the result of) a permitted use or disclosure and the use or disclosure has otherwise complied with the, in coordination with 45 CFR Parts 160 and 164 et seq.;
- disclosure required by law;
- disclosure to a public health authority;
- disclosures about victims of abuse, neglect or domestic violence;
- uses and disclosures for health oversight activities;
- uses and disclosures for judicial or administrative proceedings;
- disclosures for law enforcement purposes;
- uses and disclosures about decedents;
- uses and disclosures for cadaveric organ, eye or tissue donation purposes;
- uses and disclosures for research purposes;
- uses and disclosures to avert a serious threat to health or safety;
- uses and disclosures for specialized government functions; and
- disclosures for workers' compensation.

- Disclosures to Town's legal counsel as part of the Town's litigation and litigation avoidance strategy including accident reporting.

Notwithstanding anything in this policy to the contrary, the Plan must receive an authorization from the employee prior to using or disclosing Psychotherapy Notes, except in certain situations permitted under the HIPAA Privacy Rule.

If the Plan needs to make a use or disclosure that requires an authorization, it shall use the authorization provided in Appendix to this HIPAA Policy. The authorization shall not be valid past the date that the Plan received notice that the authorization has been revoked.

Note, that, while the use or disclosure described above may not require an authorization, 45 CFR Parts 160 and 164 et seq. may contain additional requirements for each of the items listed above.

Procedure

1. When a member of HIPAA Authorized Employees receives a request for Protected Health Information, he or she shall verify the identity of the requestor in accordance with the Verification Policy.

2. Prior to using or disclosing Protected Health Information, HIPAA Authorized Employees shall determine whether an authorization is required to make such use or disclosure pursuant to this policy and the HIPAA Privacy Rule.

3. If the use or disclosure requires neither an authorization nor an opportunity for the requesting individual to disagree or object to the use or disclosure, a member of HIPAA Authorized Employees shall refer to the HIPAA Policy or 45 CFR Parts 160 and 164 et seq. dealing with the type of use or disclosure at issue and follow the appropriate procedure for making that use or disclosure.

4. If authorization is required, the member of HIPAA Authorized Employees handling the request shall confirm receipt of an authorization and determine whether the authorization is valid under the HIPAA Policy and 45 CFR Parts 160 and 164 et seq.

5. When it is determined that the authorization is valid, HIPAA Authorized Employees may then use or disclose the Protected Health Information in accordance with the authorization.

6. If applicable, HIPAA Authorized Employees shall document the use or disclosure in accordance with the Record Retention and Documentation Policy.

7. If a valid authorization is not received, HIPAA Authorized Employees shall not use or disclose the Protected Health Information.

No employee may use or disclose information pursuant to a required authorization that has been revoked.

Disclosures Of Protected Health Information To The Town

Policy

Subject to the provisions of section 1.6 ante and in general, the Plan may not disclose Protected Health Information to the Town of West Boylston, Massachusetts.

Permitted Disclosure. Notwithstanding the foregoing, at the Town's request, the Plan may disclose:

- Summary Health Information for the purpose of obtaining premium bids for providing health insurance under the Plan or for the purpose of modifying or terminating the Plan; OR
- Enrollment and disenrollment information.

Requirements for Disclosure of Other Health Information. For a request for other Protected Health Information from the Plan other than as described above, the Plan shall not make the requested disclosure unless the Privacy Contact determines that the plan documents have been amended to:

- Establish the permitted and required uses and disclosures of such information by the Town of West Boylston, Massachusetts provided that such permitted and required uses and disclosures may not be inconsistent with the HIPAA Privacy Rule.

- Provide that the Plan shall disclose Protected Health Information to the Town of West Boylston only upon receipt of a certification by the Town of West Boylston, Massachusetts that the plan documents have been amended to incorporate the following provisions and that the Town of West Boylston, Massachusetts agrees to:

    - Not use or further disclose the Protected Health Information other than as permitted or required by the plan documents or as required by law;
    - Ensure that any agents, including a subcontractor, to whom it provides Protected Health Information received from the Plan agree to the same restrictions and conditions that apply to the Town of West Boylston, Massachusetts with respect to such information;
    - Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Town of West Boylston, Massachusetts;
    - Report to the Plan any use or disclosure of the Protected Health Information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

- Make available Protected Health Information in accordance with an employee's right to access Protected Health Information under the HIPAA Privacy Rule;
- Make available Protected Health Information for amendment and incorporate any amendments to Protected Health Information in accordance with the HIPAA Privacy Rule;
- Make available the information required to provide an accounting of disclosures in accordance with the HIPAA Privacy Rule;
- Make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from the Plan available to the Secretary for purposes of determining compliance by the Plan with this subpart;
- Return or destroy all Protected Health Information received from the Plan that the Town of West Boylston, Massachusetts still maintains in any form in accordance with HIPAA's Security Rule requirements and do not retain any 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; and
- Ensure that the adequate separation between the Plan and the Town of West Boylston, Massachusetts as required under paragraph (f) (2) (iii) of section 164.504 of 45 CFR Parts 160 and 164 et seq. as established.

Disclosures to Personal Representatives

Policy

In general, for purposes of the use and disclosure of Protected Health Information, upon written confirmation, the Plan shall treat a personal representative of an employee who is or has been a participant in the Plan in the same manner as the Plan would treat the employee.

Personal Representative of Un-emancipated Minor. In the case of an un-emancipated minor, the Plan is not obligated to treat the personal representative of such minor as the minor if:

- the minor consents to health care service and no other consent is required by law;
- the minor may lawfully obtain the health care services without the consent of a parent or guardian and the minor, the court or another authorized person consents to such health care services; or
- the parent or guardian of the minor consents to an agreement of confidentiality between the Plan and the un-emancipated minor with respect to health care services at issue.

Personal Representative of Employee. In the case of any employee, the Plan does not have to treat the personal representative of the employee as the employee if:

- the Privacy Contact reasonably believes that the employee has been or may be subject to domestic violence, abuse or neglect by the personal representative,
- the Privacy Contact reasonably believes that treating the personal representative as such could endanger the employee, or
- the Privacy Contact, in the exercise of his or her professional judgment, decides that it is not in the best interest of the employee to treat such person as the personal representative.

If the Privacy Contact determines that the Plan must make the disclosure, then the Privacy Contact shall deliver the requested Protected Health Information to the personal representative. If the Privacy Contact determines that the disclosure should not be made, the Privacy Contact or his or her designee shall notify the person making the request.

Disclosures for Judicial and Administrative Proceedings

Policy

The Plan may disclose Protected Health Information during the course of a judicial or administrative proceeding to other than a member of the HIPAA policy group:

- in response to an order of a court or administrative tribunal, OR

- in response to a subpoena, discovery request or other lawful process that is not accompanied by an order of a court or administrative tribunal IF

    - the Plan receives "satisfactory assurances" from the party seeking the Protected Health Information that such party has made reasonable efforts to ensure that the individual to whom the requested Protected Health Information relates has been given notice of the request, OR
    - the Plan receives "satisfactory assurances" from the party seeking the Protected Health Information that reasonable efforts have been made by the party seeking the Protected Health Information to secure a "qualified protective order."

Satisfactory Assurances of Reasonable Efforts to Notify. The Plan has received "satisfactory assurances" from the party requesting the Protected Health Information that such party has made reasonable efforts to ensure that the individual is notified of the request IF the Plan receives a written statement and supporting documentation demonstrating that: (1) the party has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address); (2) the notice included sufficient information about the litigation or proceeding in which the Protected Health Information is requested to permit the individual to raise an objection with the court or administrative tribunal; and (3) the time for the individual to raise objections with the court or administrative tribunal have elapsed and no objection was filed or any objection filed has been resolved and disclosure of the Protected Health Information is consistent with the resolution.

Satisfactory Assurances of Reasonable Efforts to Obtain a Qualified Protective Order. The Plan has received "satisfactory assurances" from the party requesting the Protected Health Information that reasonable efforts have been made to secure a "qualified protective order" if the Plan receives a written statement and supporting documentation demonstrating that: (1) the parties to the dispute giving rise to the request for Protected Health Information have agreed to

a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or (2) the party seeking the Protected Health Information has requested a qualified protective order from such court or administrative tribunal.

A "qualified protective order" is an order from a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (1) prohibits the parties from using or disclosing the Protected Health Information for any purpose other than the litigation or administrative proceeding for which it was sought; and (2) requires the return to the Plan or the destruction of the Protected Health Information, including all copies, at the end of the litigation or administrative proceeding.

Procedure

1. If the request is a court or administrative tribunal order, the Privacy Contact shall disclose the requested Protected Health Information and document the disclosure pursuant to the Record Retention and Disclosure Policy.

2. If the request is a subpoena or discovery request that is not accompanied by a court or administrative tribunal order, the Privacy Contact shall determine whether there is either satisfactory assurances that the requesting party has made reasonable efforts to notify the individual about whom the Protected Health Information relates or satisfactory assurances that the requesting party has made reasonable efforts to secure a qualified protective order.

    a. If such satisfactory assurances have been received, the Privacy Contact shall disclose the requested Protected Health Information and document the disclosure accordingly.

    b. If such satisfactory assurances have not been made, the Privacy Contact shall contact the Town's legal counsel to determine the Plan's obligations under the subpoena. If, after consulting with an attorney, the Privacy Contact determines that the request should be denied, the Privacy Contact so notifies the person who issued the subpoena and places the subpoena or discovery order in the Plan's files relating to denied requests for Protected Health Information.

Uses and Disclosures Required by Law

Policy

HIPAA Authorized Employees shall use and disclose Protected Health Information to the extent that the Plan is required by law to make such use or disclosure, and shall limit such use or disclosure to the relevant requirements of such law.

A use or disclosure is "required by law" under this HIPAA Policy IF it is required by statute and:

- it is made to a government authority, including social or protective services authorities, about an employee that the Plan reasonably believes is a victim of abuse, neglect or domestic violence;
- it is made in the course of a judicial or administrative proceeding in response to an order of a court or an administrative body or in response to a subpoena, discovery request or other lawful process; or
- it is made to a law enforcement official for certain law enforcement purposes, as specified in HIPAA's Privacy Rule.

Verification

Policy

If the identity or authority of a person requesting Protected Health Information is not known to the HIPAA Privacy Group, HIPAA Authorized Employees shall verify the identity and authority of the person prior to providing any access to or disclosing the Protected Health Information to the person making the request. As necessary under the HIPAA Privacy Rule, and as part of the process of verifying the identity and authority of an individual, HIPAA Authorized Employees shall receive all documentation, statements or representations necessary as a condition of the disclosure.

Verification of Identity. HIPAA Authorized Employees

Shall verify the identity of the person requesting the Protected Health Information.

- Where the disclosure is conditioned on particular documentation or representation from the requesting individual, HIPAA Authorized Employees may rely, if such reliance is reasonable, based on the face of the documents or representations themselves. The member of HIPAA Authorized Employees conducting such verification shall examine 45 CFR Parts 160 and 164 et seq. for situations where such conditions exist and apply them accordingly.

- If the person making the request is a public official, the identity of that person may be made by:

    - Viewing an agency identification badge or other proof of government employment;
    - If the request is received in writing, the request is on government letterhead; or
    - If the disclosure is to a person acting on behalf of a public official, a statement on government letterhead which states that the person is acting on behalf of a public official, or other documentation of the relationship between the individual making the request and the public official for whom the request is being made.

Verification of Authority. HIPAA Authorized Employees shall verify the authority of the person making the request to receive the Protected Health Information.

- If the request is made by a public official, authority may be verified:

- By a written or oral statement of legal authority; or
- By viewing the warrant, subpoena, order or other legal process pursuant to which the request is being made.

If required, the appropriate member of HIPAA Authorized Employees shall document the disclosure pursuant to Record Retention and Documentation Policy.

Notice of Privacy Practices

Policy

It is a violation of the HIPAA Policy to use or disclose Protected Health Information in a manner, which is inconsistent with the Notice of Privacy Practices then in effect. (The Notice of Privacy Practices is set forth in the Forms and Notices Section of this HIPAA Policy.).

The Privacy Contact shall provide the Notice of Privacy Practices at all times and in such manner as is required under 45 CFR Parts 160 and 164 et seq. In the event that an employee determines that the privacy practices contained in the Notice of Privacy Practices should be changed for any reason, the employee shall notify the Privacy Contact. The Privacy Contact shall review the employee's determination and, if necessary, cause the Notice of Privacy Practices to be modified in accordance with the procedures set forth in the policy entitled, "Amending the HIPAA Policy" and redistributed according to this policy.

The Privacy Contact shall cause the Notice of Privacy Practices to be distributed to necessary individuals at all times and in the manner required under the HIPAA Privacy Rule. Unless 45 CFR Parts 160 and 164 et seq. provides otherwise:

- All employees that participate in the Plan shall receive a Notice of Privacy Practices on or before the date, the Plan first becomes subject to 45 CFR Parts 160 and 164 et seq. and thereafter as a standard part of enrollment in the Plan.
- In the event of a material change in the HIPAA Policy, all employees then covered under the Plan shall be provided with a revised Notice of Privacy Practices within 60 days of the material revision.
- Every three years, the Privacy Contact shall notify all employees then covered of the availability of the Notice of Privacy Practices and how to obtain it.

Any employee who uses or discloses Protected Health Information in violation of this HIPAA Policy or 45 CFR Parts 160 and 164 et seq. shall be subject to the DISCIPLINARY PROCEDURES of Town of West Boylston, Massachusetts, which may include termination as well as civil or criminal penalties.

De-Identified Information

Policy

If Protected Health Information is converted by HIPAA Authorized Employees to "de-identified" information in accordance with this HIPAA Policy and 45 CFR Parts 160 and 164 et seq. the converted information will no longer be subject to this HIPAA Policy or the 45 CFR Parts 160 and 164 et seq. Protected Health Information is converted into de-identified information if: (1) certain specific identifiers are removed; and (2) the Plan does not know that the remaining information can be used to identify an individual (either alone or in combination with other information).

To convert Protected Health Information to de-identified information, the following identifiers that relate to individuals, employees, their relatives, other household members or employers must be removed:

- Names of individuals.
- Geographic units -- all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and their equivalent geo-codes. However, the initial three digits of a zip code may be used if, according to Census Bureau data, the geographic unit formed by combining all Zip Code Tabulation Areas (ZCTAs) with the same three initial digits has more than 20,000 people, and the initial three digits of all such geographic units with 20,000 or fewer people are changed to 000. Results of the 2000 Census indicate that only 17 three-digit ZCTAs have fewer than 20,000 people.
- Dates -- any month or day directly related to an individual, including birth date, admission date, discharge date and date of death. However, listing an individual's age is broad enough to be allowed in de-identified information (subject to the exception for individuals age 90 or older described below).
- Ages -- all those over 89 and any combination of month, day or year that reveals an individual's age to be over 89, because nonagenarians are relatively rare. However, ages and identifying dates (month, day and year) of several individuals may be aggregated into a single category of age 90 or older.
- Telephone numbers.
- Fax numbers.
- E-mail addresses.
- SSNs.
- 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) addresses numbers.
- Biometric identifiers, including finger and voiceprints.
- Full face photographic images and any comparable images.
- Any other unique identifying number, characteristic or code, except a re-identification code.

Example: A plan sponsor will often receive reports from a self-insured plan that provide important information about health plan utilization and costs. Under the HIPAA Privacy Rule, the reports may have information such as an individual's age, gender, race, ethnicity and marital status, as well as some geographic location information. These reports still will be de-identified. However, if birth dates, admission dates and other date-specific information -- as well as identifying numbers (such as SSN) -- are shown, then the information is not de-identified. To become de-identified, the dates and numbers must be eliminated and zip codes must be limited to only the first three digits (and in some rural areas must be aggregated even further). A plan sponsor may receive reports with PHI that has not been de-identified if it has amended its plan documents based on the HIPAA Privacy Rule.

POLICIES REGARDING THE RIGHTS OF INDIVIDUALS UNDER 45 CFR Parts 160 and 164 et seq.

Access to Protected Health Information

Policy

Generally, every individual has the right to inspect and obtain a copy of his/her own Protected Health Information that is maintained by the Plan in accordance with the following procedures:

1. All requests for access to Protected Health Information shall be made by an employee or his or her duly authorized representative shall be made in writing to HIPAA Authorized Employees using the form attached in the Forms and Notices Section of this HIPAA Policy.

2. The HIPAA Policy Groups shall respond to all requests for access within 10 days of receipt of the request. If HIPAA Authorized Employees is unable to respond within either period, it shall seek an extension of time to respond by notifying the requestor (within the respective periods mentioned in the preceding sentence) in writing of the reasons for the delay and the date it will make its determination.

3. A request for access to Protected Health Information may be denied if:

   - The Protected Health Information requested was compiled in reasonable anticipation of a civil, criminal or administrative action (e.g. lawsuits and similar proceedings);
   - The Protected Health Information requested is subject to the Privacy Act, 5 USC Sec. 552; or
   - The Protected Health Information requested was obtained from someone other than a health care provider under a promise of confidentiality and the access would likely reveal the source.

   If it is determined, under this policy, that access to the requested Protected Health Information must be denied because of one or more of the reasons set forth above, that determination shall not be subject to review at the request of the employee or his or her duly appointed representative.

4. In certain cases, the determination to deny access to Protected Health Information may be reviewed by the employee or his or personal representative. Those situations, as set forth in 45 CFR Parts 160 and 164 et seq. are incorporated herein by reference. In these cases, the HIPAA Policy Groups hall provide for a review of the determination pursuant to the HIPAA Privacy Rule.

5. If it is determined under this policy that access to the requested Protected Health Information must be provided to the employee, HIPAA Authorized Employees shall notify the employee or his or her duly authorized representative in writing that the request has been granted and provide the Protected

Health Information to the requesting employee or his or her duly appointed representative at a convenient time or location and in the form requested, unless such form is not readily producible and then in hard copy or another form mutually agreeable to the employee and the HIPAA Privacy Group.

6. HIPAA Authorized Employees may impose a reasonable, cost-based, fee which shall include only the cost of: (i) copying the Protected Health Information, including the supplies and labor involved; (ii) postage for mailing the Protected Health Information; and (iii) if agreed to with the requesting individual the cost of preparing an explanation or summary of the Protected Health Information.

7. In any case, in which access to the requested Protected Health Information is denied, HIPAA Authorized Employees shall, to the extent possible, provide access to any other Protected Health Information requested that is not part of the Protected Health Information that the Plan has grounds to deny access. With respect to the Protected Health Information to which the Plan denies access, HIPAA Authorized Employees shall notify the requesting employee or his or her duly appointed representative of the denial in a writing that states:

   - The basis for the denial;
   - If applicable, a statement that the employee may have the right to have a licensed health care professional, chosen by the Plan, review the decision to deny access to the Protected Health Information including a description of how the individual may exercise such review rights;
   - The procedure by which the requesting employee or his or her duly appointed representative may file a complaint with the Plan and the title and telephone number of the person with whom the complaint can be filed; and
   - The procedure by which the requesting employee or his or her duly appointed representative may file a complaint with the Plan or the Secretary of Health and Human Services.

8. If the denial of access is subject to review under number 4 above and the requesting employee or his or her duly appointed representative requests a review, HIPAA Authorized Employees shall appoint a licensed health care professional not involved in the original decision to deny access to review the request. HIPAA Authorized Employees and the requesting employee or his or her duly appointed representative are bound by the determination made by the reviewing health care professional.

9. HIPAA Authorized Employees shall document the Designated Record Sets that are subject to review and the titles of the persons or offices responsible for receiving and processing requests for access.

Amendments of Protected Health Information

Policy

Employees of the Plan have the right to request that the Plan amend Protected Health Information or a record about the employee in a Designated Record Set for so long as such Protected Health Information or record exists in a Designated Record Set. The Plan may only deny the employee's request to have his or her Protected Health Information or a record amended if:

- the Protected Health Information or record was not created by the Plan, unless the employee provides a reasonable basis to believe that the originator of the Protected Health Information is no longer available to amend it,
- it is not part of a Designated Record Set,
- the employee does not have the right to inspect the Protected Health Information which he or she is requesting to have amended, as set forth in Access to Protected Health Information policy, or
- the Protected Health Information is accurate and complete.

All requests for an amendment of Protected Health Information must be made in writing to HIPAA Authorized Employees using the form attached in the Forms and Notices Section of this HIPAA Policy. The request shall include a reason that supports the requested amendment. If the amendment request applies to Protected Health Information not contained in the Plan's Designated Record Set and not otherwise, in the possession of the Town of West Boylston, Massachusetts or the Plan, no amendment shall be required.

The Plan, through the HIPAA Privacy Group, shall attempt to act on every request for an amendment within 60 days of receiving the request in accordance with the following:

1. If the Plan grants the requested amendment:
   - The Plan shall make the appropriate amendment to the Protected Health Information or record that is the subject of the request by identifying the Protected Health Information or records that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
   - The Plan shall notify the employee that the amendment was accepted and shall obtain from the employee the identification of those persons with whom the amendment should be shared, and authorization to share such amendment.

- The Plan shall make reasonable efforts to inform and provide the amendment within a reasonable time to: (i) persons identified by the employee as having received Protected Health Information about the employee and needing the amendment; and (ii) persons, including Business Associates, that the Plan knows have Protected Health Information which is the subject of the amendment and that may have relied, or could foreseeably rely, on the Protected Health Information to the detriment of the employee.

2. If the Plan denies the requested amendment:

- The Plan shall provide a written denial to the employee which contains:

    - the basis for the denial,
    - a statement that the employee has the right to submit a written statement disagreeing with the denial and how the employee may file such a statement,
    - a statement that if the employee does not submit a statement of disagreement, the employee may request that the Plan provide the employee's request for amendment and the denial with future disclosures of the Protected Health Information that is the subject of the request, and
    - a description on how the employee may file a complaint with the Plan in accordance with the Complaint Policy or to the Secretary of HHS. This description shall contain the name or title, and telephone number of the Plan's contact person.

- The employee may file a written statement of reasonable length setting forth the basis for his or her disagreement with the denial of the request for amendment.

    - If the employee files a written statement, disagreeing with the denial of the request for amendment the Plan may prepare a written rebuttal to the employee's statement of disagreement. The Plan shall provide a copy of the rebuttal to the employee.
    - The Plan shall, as appropriate, identify the record or Protected Health Information in the Designated Record Set that is the subject of the disputed amendment and append, or otherwise link the employee's request for an amendment, the Plan's denial of the request, the employee's statement of disagreement, if any, and the Plan's rebuttal, if any, to the Designated Record Set.
    - In the case of future disclosures of Protected Health Information with respect to which the employee filed a statement of disagreement, the Plan shall include the material

appended as described in the preceding paragraph or, as the Plan may elect, an accurate summary of such information. If the employee submitted no statement of disagreement, the Plan shall, only at the request of the employee, include a copy of the request for amendment and statement of denial, or a summary thereof, with disclosures of the Protected Health Information to which the amendment relates. If the future disclosure is made using a standard transaction that does not permit the disclosure of additional material to be included with the disclosure, the Plan shall separately transmit the appended information to the recipient of the standard transaction.

3. If the Plan is unable to act on the requested amendment within 60 days of receipt, the Plan shall inform the employee within the 60-day period by providing a written notice containing the reasons for the delay and the date on which the Plan will complete its action on the request. The Plan may not extend the time for action by more than 30 days and may extend the time for action only once for each request for amendment received.

4. If the Plan is informed of an amendment to an employee's Protected Health Information by another plan, the Plan shall amend the employee's Protected Health Information in accordance with the procedure by which the Plan amends Protected Health Information if a request for amendment is accepted.

5. The Plan shall document the title of the person or office responsible for receiving and processing requests for amendments by an employee and shall retain such documentation in accordance with the Record Retention and Documentation Policy.

Complaints

Policy

The HIPAA Policy Group shall receive, document and investigate every complaint that an individual makes regarding the HIPAA Policy or use or disclosure of his or her Protected Health Information. Any such complaint shall be filed with the Privacy Contact, or such person or persons who may be designated by the Privacy Contact for this purpose (the "Complaint Investigator").

Complaints shall be made in writing to the HIPAA Privacy Group. A form for complaints is attached in the Forms and Notices Section of this HIPAA Policy.

All complaints shall be investigated. If it is determined that there has been a violation of 45 CFR Parts 160 and 164 et seq. or this HIPAA Policy, the Privacy Contact shall take any action required under the Mitigation Policy, the Sanctions Policy, or the HIPAA Privacy Rule, as applicable.

At no time will an employee who is the subject of a complaint be the same person in charge of investigating the complaint.

An individual may also file a Complaint directly with the U.S. Health and Human Services Office of Civil Rights.

Procedure

1. The Complaint Investigator shall accept only written complaints.

2. The Complaint Investigator shall document the complaint process and all actions taken with respect thereto according to the Record Retention and Documentation Policy.

3. The Complaint Investigator shall review all available information relating to the use or disclosure of the complaining individual's Protected Health Information, including all written documentation relating to the use and disclosure of such Protected Health Information.

4. If the Privacy Contact agrees with the Complaint Investigator's determination, the Privacy Contact shall sanction the employee responsible for the inappropriate use or disclosure of the Protected Health Information in accordance with the Sanction Policy. If necessary, the Privacy Contact shall take steps to mitigate the effects of an inappropriate use or disclosure in accordance with the Mitigation Policy. The Privacy Contact shall document the action taken and place all information relating to the employee's complaint in the Complaint File.

5. If Complaint Investigator determines that the complaint has no merit, the investigation made is documented and placed in the Complaint File.

6. In the event that the complaint is about the Complaint Investigator, the complaint shall be handled by Privacy Contact. In the event that the complaint is about the Privacy Contact or the Complaint Investigator and Privacy Contact, the complaint shall be handled by the West Boylston Town Administrator **according** to this Complaint Policy.

Confidential Communications of Protected Health Information

Policy

An employee may request that the Plan communicate Protected Health Information to him or her by alternative means or at alternative locations. The Plan acting through members of HIPAA Authorized Employees shall accommodate all such requests that are reasonable in the discretion of the Privacy Contact.

Any request for confidential communications shall be made in writing to the HIPAA Privacy Group. A form for such request is attached in the Forms and Notices Section of this HIPAA Policy.

A member of HIPAA Authorized Employees shall accommodate such a request only after the employee provides an alternative address or method of contact and, when necessary and appropriate, information on how payment will be handled. The Plan shall not require the employee to explain why he or she is seeking such an accommodation.

Procedure

1. If the request is determined to be reasonable, within the discretion of the Privacy Contact, and the Plan is capable of accommodating the request, the Privacy Contact or his or her designee shall:

    - notify employee that reasonable accommodation will be made;
    - if necessary and appropriate, discuss how payment will be handled while accommodation is being made;
    - if not already included in the employee's request, ask the employee to provide an alternative address or method of contact;
    - document the location at which or the manner by which Protected Health Information is to be communicated and place the documentation in the employee's Protected Health Information File; and
    - inform relevant Business Associates of the request and the alternate means and/or locations of providing confidential communications.

2. If the Privacy Contact determines that the request is unreasonable and the Plan is unable to make such an accommodation, the Privacy Contact shall notify the employee of the decision.

Documenting Disclosures and Accountings

Policy

Generally, within 60 days of receiving a request from an employee or his or her duly authorized representative, the Privacy Contact, or his or her designee, shall provide an accounting of all documented disclosures of Protected Health Information that have been made during the period for which the accounting was requested. The accounting period cannot exceed the six (6) years prior to the date on which the request for an accounting was received. An accounting need not include any disclosure that the Plan is not required to document under the HIPAA Privacy Rule. All requests to account for disclosures of Protected Health Information shall be in writing to the HIPAA Privacy Group. A form for such requests is attached in the Forms and Notices Section of this HIPAA Policy.

Procedure – Documenting Disclosures

1. Except as otherwise provided in paragraph 3 below, when Protected Health Information is disclosed, the disclosure shall be recorded in the Protected Health Information Disclosure Log.

2. Every record of a disclosure shall include:

   - The date the disclosure was made;
   - The name and, if known, the address of the entity or person who received the Protected Health Information;
   - A brief description of the Protected Health Information disclosed; and
   - A brief statement of the purpose for the disclosure which reasonably describes the basis on which the disclosure was made or a copy of the written request for disclosure.

3. A disclosure need not be documented if the disclosure was made:

   - To carry out Treatment, Payment or Health Care Operations;
   - To the individual about whom the Protected Health Information relates;
   - Incident to an otherwise permissible disclosure under the HIPAA Privacy Rule;
   - Pursuant to an authorization given by the employee;
   - For national security reasons or intelligence purposes;
   - To a correctional facility or to law enforcement officials;

- As part of a limited data set; or
- Prior to the compliance date of 45 CFR Parts 160 and 164 et seq. for the Plan.

Procedure – Accounting For Disclosures

4. The Privacy Contact, or his or her designee, shall, to the extent possible, prepare the requested accounting within 60 days of receiving the request.

5. The accounting prepared shall include the following information relating to all documented disclosures made during the accounting period, which period may not exceed the 6 years prior to the date on which the request for an accounting was received:

   - The date of the disclosure;
   - The name and, if known, the address of the person to whom the disclosure was made;
   - A brief description of the Protected Health Information which was disclosed; and
   - A brief statement of the purpose for the disclosure, which reasonably sets forth the basis upon which the disclosure was made.

6. If the requested accounting cannot be provided within 60 days of receiving the request, the Privacy Contact may extend the time period for providing the accounting by 30 days provided the Privacy Contact, or his or her designee, during the initial 60-day period, notifies the requestor of the reasons for the delay and indicates when the accounting shall be provided.

7. If during the same 12-month period the same individual makes more than one request for an accounting, the Privacy Contact may impose a reasonable cost-based fee with respect to each request provided that the Privacy Contact provides the individual with: (i) advance notice of the fee; and (ii) an opportunity to withdraw the request to avoid or reduce the fee. The fee shall be calculated in the same manner as under the Access to Protected Health Information Policy.

8. The Privacy Contact shall suspend the requestor's right to an accounting if the Plan is notified by a health oversight committee or law enforcement agency that making an accounting would impede such agency's activities.

   - If notified in writing, the right to an accounting shall be suspended for the period set forth in the notification from the agency.
   - If notified orally, the right to an accounting shall be suspended for no longer than 30 days, unless the appropriate agency subsequently provides notice in writing.

- The Privacy Contact shall document this suspension accordingly, and inform the requestor of such suspension.

Requesting Restriction On Uses and Disclosures OF Protected Health Information

Policy

The Plan shall allow any individual to request a restriction on the uses and disclosures of Protected Health Information made on behalf of the Plan about the employee to carry out Treatment, Payment or Health Care Operations. Additionally, the Plan shall allow any employee to request a restriction on the disclosure of Protected Health Information about the employee to a family member, other relative, close personal friend or other person designated by the employee relating to such person's involvement with the employee's care or payment for the employee's health care or to inform a family member, other relative, close personal friend or other person responsible for the care of the employee about the employee's location, general condition or death.

Any request for a restriction shall be made in writing to the HIPAA Privacy Group. A form for such requests is attached in the Forms and Notices Section of this HIPAA Policy.

If the Privacy Contact, on behalf of the Plan, agrees to any requested restriction, the Protected Health Information shall not be used or disclosed in violation of the restriction, except to the extent such Protected Health Information is necessary to provide the emergency treatment to the employee or other purposes permitted under the HIPAA Privacy Rule, despite the existence of a restriction to the contrary. An approved restriction may only be terminated pursuant to the HIPAA Privacy Rule.

Procedure

1. HIPAA Authorized Employees shall review and respond to all restriction requests. Such responses shall be subject to review by the Privacy Contact. All cases denying the restriction request must be approved by the Privacy Contact.

2. Following a review of a restriction request, the Privacy Contact or his designee shall inform the employee whether the Plan has agreed to the restriction requested.

3. If the restriction request is approved, the Privacy Contact shall maintain a copy of the request for restriction in the employee's Protected Health Information File and in the Active Restriction File. Notation shall be made where necessary, electronic or otherwise, to ensure that the restriction is followed.

4. If the restriction request is not approved, the Privacy Contact shall maintain a copy of the request for restriction in the employee's PHI File.

5. If the Privacy Contact agrees to a restriction, the employee's Protected Health Information may not be used or disclosed in violation of the restriction, except as provided in this HIPAA Policy.

GENERAL POLICIES

Interpretation and Application of the HIPAA Policy

Subject to the approval of the Town Administrator

The Privacy Contact shall have authority and discretion to resolve any questions or disputes concerning the interpretation or application of the provisions of this HIPAA Policy or 45 CFR Parts 160 and 164 et seq. subject to applicable requirements of law.

Amending the HIPAA Policy

Policy

Subject to the approval of the West Boylston Town Administrator, The Privacy Contact has the right to make material changes to this HIPAA Policy and to apply those changes to all Protected Health Information maintained by the Plan. When a material change is made in the HIPAA Policy, such change shall conform to the requirements of 45 CFR Parts 160 and 164 et seq. and a corresponding change shall be made to the Notice of Privacy Practices. No material change in the HIPAA Policy shall be implemented until all employees then covered under the Plan receive an updated Notice of Privacy Practices incorporating the change(s) made. The revisions to the HIPAA Policy shall become effective on the effective date as set forth in the new Notice of Privacy Practices.

The Privacy Contact shall conform the Plan's Training Program to the changes in the HIPAA Policy.

Mitigation of Known Violations of the HIPAA Policy

Policy

Subject to HIPAA's breach notification requirements, the Privacy Contact shall mitigate, to the extent possible, any harmful effect of a use or disclosure of Protected Health Information that is known to the Privacy Contact or any member of HIPAA Authorized Employees to be in violation of the HIPAA Policy or 45 CFR Parts 160 and 164 et seq.

- The Privacy Contact shall review all information available relating to the violation and determine what actions should be taken to minimize the harmful effects of the violation.

- The Privacy Contact shall take appropriate actions to mitigate the harmful effects of the violation and document all mitigating actions taken pursuant to the Record Retention and Documentation Policy. The Privacy Contact shall require further training to the extent deemed necessary to prevent further violations of a similar nature.

Record Retention and Documentation Policy

Policy

The Plan shall maintain this HIPAA Policy and any changes thereto in written or electronic form. The Plan shall maintain a copy, in written form or electronically, of any communication required under this HIPAA Policy or the HIPAA Privacy Rule. Similarly, the Plan shall keep a written or electronic record of any action, activity or designation that is required to be documented under the HIPAA Privacy Rule. The Plan shall develop a system to maintain such documentation required by 45 CFR Parts 160 and 164 et seq. for the longer of seven years from the date of its creation or seven years from the date when it was last in effect.

Procedure

1. The following actions involving the use and disclosure of Protected Health Information, as well as any other instances specified in the HIPAA Privacy Rule, shall be documented by the appropriate member of the HIPAA Privacy Group:

    - Satisfactory assurances of Business Associates
    - Authorizations
    - Support for a disclosure with respect to a judicial or administrative procedure
    - As necessary under the Verification Policy
    - Providing the Notice of Privacy Practices
    - Implementation of restrictions on Protected Health Information
    - Subjecting a Designated Record Set to access
    - Designations in general, including designations of persons to handle requests for restrictions, accounting and access to Protected Health Information
    - Agency or official's oral statement requiring temporary suspension of individual's right to account for Protected Health Information
    - Disclosures under this HIPAA Policy as required under the Documenting Disclosures and Accounting Policy
    - Training efforts of the Plan
    - All complaints and the dispositions of the complaints
    - Breach notifications
    - Sanctions applied for violations

- Changes made to the HIPAA Policy
- Designation as a hybrid entity
- Designation of an affiliated entity

2. Any correspondence that is received by an employee of Town of West Boylston, Massachusetts other than a member of HIPAA Policy Group shall immediately be dated with the date of the receipt and forwarded to the HIPAA Privacy Group, without retaining a copy of such correspondence.

3. Such documentation, including correspondence involving Protected Health Information, shall be maintained in secured file cabinets dedicated solely to maintaining records and documentation under the HIPAA Privacy Rule. No other files, records or documentation of any kind shall be commingled with Protected Health Information or the records required to be documented and maintained under the HIPAA Privacy Rule. Only members of HIPAA Authorized Employees shall have access to such cabinets.

4. In the event Protected Health Information or documentation is stored electronically, only members of HIPAA Authorized Employees shall have access to such files, which shall be securely maintained. The Privacy Contact shall cause to be put in place reasonable technological safeguards, such as establishing passwords or adjustments to network access or other means, to secure such files.

5. In the event an employee is no longer a member of the HIPAA Privacy Group, such person shall be required to surrender any key or other means of access to the documentation or Protected Health Information maintained by the Plan (e.g., keys to file cabinets). In addition, all means of access to electronic files shall be eliminated with respect to such person, such as changing the passwords granting access to such information.

6. From time to time, the Privacy Contact shall review the documentation and Protected Health Information maintained by the Plan and destroy any such materials no longer required to be maintained under this HIPAA Policy.

Refraining from Intimidating Or Retaliatory Acts

Policy

the Town of West Boylston shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any employee for exercising any of his or her rights under the HIPAA Privacy Rule. In addition, the Town of West Boylston shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any employee or other person for:

- filing a complaint with the Secretary of HHS;
- testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
- opposing any act or practice that is unlawful under HIPAA Privacy Rule, provided the individual has a good faith belief that the practice to which he/she is opposed is indeed unlawful, and that the manner in which he/she voices his/her opposition is reasonable, and does not itself involve a disclosure of Protected Health Information that would violate the HIPAA Privacy Rule.

Procedure

1. The Privacy Contact shall, as part of each employee's training, notify each employee that he or she may not retaliate against any individual for exercising any right such individual holds under the HIPAA Privacy Rule.

2. If an employee becomes aware of, in any manner, a retaliatory act taken by any employee of the Town of West Boylston, such employee shall immediately notify the Privacy Contact.

3. The Privacy Contact shall follow the procedure for sanctioning the employee(s) responsible for the retaliatory or intimidating act.

Sanctions

Policy

The Town of West Boylston shall apply appropriate sanctions against any employee or other member of its workforce who fails to comply with the HIPAA Policy implemented by the Plan through the HIPAA Policy Group, or who otherwise violates any federally or state mandated security or privacy rules.

Such sanctions shall NOT apply in the event of:

- A disclosure by a member of the Town of West Boylston workforce or a Business Associate of the Town, provided: (i) the workforce member or Business Associate believes in good faith that Town of West Boylston or the Plan, or a person acting on behalf of either Town of West Boylston or the Plan, has engaged in conduct that is unlawful; and (ii) the disclosure is to a health oversight agency or public health authority authorized to oversee the relevant conduct, or to an attorney retained by or on behalf of the workforce member or Business Associate for the purpose of determining the legal options with respect to such conduct.

- A disclosure of Protected Health Information by a member of the Town of West Boylston who is a victim of a criminal act to a law enforcement official, provided that: (i) the Protected Health Information is about the suspected perpetrator of the criminal act; and (ii) the Protected Health Information disclosed includes ONLY:

    - Name and address;
    - Date and place of birth;
    - Social security number;
    - ABO blood type and rh factor;
    - Type of injury;
    - Date and time of treatment;
    - Date and time of death; and
    - Distinguishing characteristics such as height, weight, gender, race, hair, eye color, presence or absence of facial hair, scars and tattoos.

Sanctions also shall NOT apply to any other individual or person who:

- Files a complaint with the Secretary of HHS;

- Testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

- Opposes any act or practice that is unlawful under the HIPAA security regulations or the HIPAA Privacy Rule, provided the individual has a good faith belief that the practice to which he/she is opposed is indeed unlawful, and that the manner in which he/she voices his/her opposition is reasonable, and does not itself involve a disclosure of Protected Health Information that would violate the HIPAA security regulations or the HIPAA Privacy Rule.

Procedure

1. Any member of the Town of West Boylston's workforce that knows or reasonably suspects that there has been a violation of the HIPAA Policy or 45 CFR Parts 160 and 164 et seq. shall report the suspected violation to the HIPAA Policy Group or the HHS Office of Civil Rights.

2. The Privacy Contact shall review the facts surrounding the reported violation to determine whether the HIPAA Policy or 45 CFR Parts 160 and 164 et seq. has been violated.

3. If the Privacy Contact determines that there has been a violation of the HIPAA Policy or 45 CFR Parts 160 and 164 et seq. the Privacy Contact shall determine whether the alleged violation occurred in the context of:

   - "whistle-blowing";
   - A workforce member who was the victim of a crime;
   - The filing of a complaint with the Secretary of Health and Human Services;
   - Participation in an investigation under Part C, Title XI, as noted above; or
   - Or in opposition to an act that the workforce member believed, in good faith, to be a violation of the employee's privacy rights, provided that the actions of the workforce member in voicing his/her opposition were reasonable and did not violate the employee's privacy rights.

4. In the event that the HIPAA Policy or 45 CFR Parts 160 and 164 et seq. is violated, the Privacy Contact shall undertake, to the extent practicable, any reasonable measures available to the Privacy Contact

in order to mitigate (lessen) any harmful effect of the violation of the HIPAA Policy or 45 CFR Parts 160 and 164 et seq. and shall document any action taken.

5. The Privacy Contact shall report the facts surrounding the reported violation to the Town Administrator and other appropriate persons within the Town of West Boylston pursuant to its disciplinary procedures, including the employee's immediate supervisor.

6. The appropriate level of sanction shall be applied pursuant to Town of West Boylston's disciplinary procedures.

7. The Privacy Contact shall document any sanctions imposed on the employee, and such documentation shall be retained in the employee's personnel record provided such documentation does not include Protected Health Information.

8. Any modifications to this policy and/or the disciplinary procedures to which this policy is subject shall be communicated to all the Town of West Boylston employees at the time such modifications become effective.

Training Policy

Policy

The Plan shall cause all members of HIPAA Authorized Employees to receive training in the requirements of this HIPAA Policy and the HIPAA Privacy Rule. As necessary in the determination of the Privacy Contact, this training or training to a lesser degree may be provided to some or all of the employees of the Town. The training shall be that which is necessary and appropriate for each employee to carry out his or her job. Following the initial training, additional training shall be provided, as necessary and appropriate within the Privacy Contact's determination, for the purpose of reminding some or all of the employees about certain aspects of 45 CFR Parts 160 and 164 et seq. and this HIPAA Policy, and to train such individuals with respect to changes in such policies.

GLOSSARY

Business Associate

1. Except as provided in paragraph (2) of this definition, Business Associate means, with respect to a Covered Entity, a person who:

    - On behalf of such Covered Entity or of an organized health care arrangement (as defined in § 164.501 of the HIPAA Privacy Rule) in which the Covered Entity participates, but other than in the capacity of a member of the workforce of such Covered Entity or arrangement, performs, or assists in the performance of:

        - A function or activity involving the use or disclosure of Individually Identifiable Health Information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
        - Any other function or activity regulated by this subchapter;

    OR

    - Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of Individually Identifiable Health Information from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

2. A Covered Entity participating in an organized health care arrangement that performs a function or activity or service, as described by paragraph 1 of this definition, for or on behalf of such organized health care arrangement does not, simply through the performance of such function or activity or the provision of such service, become a Business Associate of other Covered Entities participating in such organized health care arrangement.

3. A Covered Entity may be a Business Associate of another Covered Entity.

Covered Entity

means

- A health plan;

- A health care clearinghouse; or

- A health care provider who transmits any Health Information in electronic form in connection with a Transaction.

Designated Record Set

Means a group of records maintained by or for a Covered Entity that is:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the Covered Entity to make decisions about individuals.

For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity.

Health Information

means any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future Payment for the provision of health care to an individual.

Individually Identifiable Health Information

is information that is a subset of Health Information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future Payment for the provision of health care to an individual; and
- That identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Health Care Operations

means any of the following activities of the Covered Entity to the extent that the activities are related to covered functions:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of general knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of 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;

- Underwriting, 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 (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) of, in coordination with 45 CFR Parts 160 and 164 et seq. are met, if applicable;

- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

- Business management and general administrative activities of the entity, including, but not limited to:

    - Management activities relating to implementation of and compliance with the requirements of this subchapter;

    - Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that Protected Health Information is not disclosed to such policyholder, plan sponsor, or customer.

    - Resolution of internal grievances;

    - The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and

- Consistent with the applicable requirements of § 164.514 of the HIPAA Privacy Rule, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity.

Payment

means:

1. The activities undertaken by:

   - A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

   - A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

2. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

   - Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
   - Risk adjusting amounts due based on enrollee health status and demographic characteristics;
   - Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
   - Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
   - Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
   - Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement:

     - Name and address;
     - Date of birth;
     - Social security number;
     - Payment history;
     - Account number; and
     - Name and address of the health care provider and/or health plan.

Plan Administration Functions

means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Protected Health Information

means Individually Identifiable Health Information:

1. Except as provided in paragraph (2) of this definition, that is:

   - Transmitted by electronic media;
   - Maintained in any medium described in the definition of electronic media at § 162.103 of the HIPAA Privacy Rule; or
   - Transmitted or maintained in any other form or medium.

2. Protected Health Information excludes Individually Identifiable Health Information in:

   - Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
   - Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
   - Employment records held by a plan sponsor in its role as employer.

Psychotherapy Notes

means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. ***Psychotherapy notes*** excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Summary Health Information

means information, that may be Individually Identifiable Health Information, and:

- That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

- From which the information described at § 164.514(b) (2) (i) of, in coordination with 45 CFR Parts 160 and 164 et seq. has been deleted, except that the geographic information described in § 164.514(b) (2) (i) (B) of, in coordination with. 45 CFR Parts 160 and 164 et seq. need only be aggregated to the level of a five-digit zip code.

Town of West Boylston

means **The Town of West Boylston Massachusetts**

Transaction

means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

- Health care claims or equivalent encounter information.

- Health care payment and remittance advice.
- Coordination of benefits.
- Health care claim status.
- Enrollment and disenrollment in a health plan.
- Eligibility for a health plan.
- Health plan premium payments.
- Referral certification and authorization.
- First report of injury.
- Health claims attachments.
- Other transactions that the Secretary may prescribe by regulation.

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.

APPENDIX

Plans and Programs Covered By This HIPAA Policy

The health plans and programs sponsored or operated by the Town of West Boylston including:

- **List all health plans)**
- **Town of West Boylston EMS**

Privacy Contact and HIPAA Policy Group Designations

Privacy Contact:

Name: (name and or title) shall serve as Privacy Contact.

Reports to: The Privacy Contact shall report to the Town Administrator

HIPAA Privacy Group

The following persons are members of HIPAA Authorized Employees referred to at Section 1.1 of the HIPAA Policy:

- Privacy Contact;
- Designees of the Privacy Contact; and
- (list HIPAA Group by name and Title)
- The following positions have access to payroll health insurance premium deduction records only (List designated employees and position title)

- The following IT personnel have access to all stored e-phi:
  Information Technology Director, Network Administrator

Specific Rules for Access and Use of Protected Health Information

Only HIPAA Policy Group members are permitted to handle Protected Health Information. All HIPAA Policy Group members shall ensure that any employees working under their supervision have a general understanding of the HIPAA Policy's requirements. Such employees should be instructed to immediately forward to HIPAA Authorized Employees and retain no copies of any information likely to be Protected Health Information. Except as further limited below, only HIPAA Policy Group members shall have access to Internet websites provided by service providers to monitor benefits administration and payment.

Website Administration. Any benefit elections or changes to the benefits of a participant in one of the Town's group health plans to be made, if applicable, through the secured website shall be made only by a member of the HIPAA Privacy Group. Records of such changes shall be kept, as directed by the Privacy Contact, in the participant's PHI file, as described below.

Mail/Telephone/Email Policies. The following procedures apply to the transfer of Protected Health Information via either regular mail, private courier, or other similar means; telephonically; and email or other electronic means:

- HIPAA Policy Group members shall direct their respective employees who receive mail that may relate to or be Protected Health Information to forward that information directly to the appropriate service provider or HIPAA Policy Group member.

- All incoming mail that is not addressed to any person's attention shall not be opened and shall be immediately forwarded to the Treasurer/Collector's office. In the event the addressee is unreadable, the mailroom administrator shall forward that article to the Privacy Contact.

- All mail that is marked "Personal and Confidential" and addressed to an individual shall be forwarded to that individual unopened.

- All outgoing mail, including inter-office mail, containing Protected Health Information shall be sealed before it is sent to the mailroom.

- Any non-HIPAA Policy Group member receiving a telephone call involving Protected Health Information shall be instructed to immediately inform the caller that he or she is not permitted

to discuss Protected Health Information and direct the caller to contact the appropriate service provider or HIPAA Policy Group member.

- All outgoing email, which includes or is likely to include Protected Health Information, shall contain the following disclaimer: *"This correspondence may contain protected health information subject to the federal privacy rule, 45 C.F.R. pts. 160 and 164 and state law. Unauthorized use or disclosure of this information is strictly prohibited and may be subject to fines and other penalties. If you have received this correspondence in error, please destroy immediately."*

File management. HIPAA Policy Group members shall keep and maintain Protected Health Information in locked file cabinets to which only they have access. In addition, to the extent any such information is maintained electronically, the electronic files shall be password protected and, if necessary, otherwise secured in a commercially reasonable manner by encryption.

These "PHI files," whether in hard copy or electronic, shall include only Protected Health Information. That is, these PHI files shall be kept in separate file cabinets or file cabinet drawers and shall not include employment records or information even if the record or information is health related, such as in the case of records related to FMLA certification, disability claims, doctor's notes for personal leave, etc.

All questions regarding whether a record or information is Protected Health Information shall be resolved by the Privacy Contact. In the event Protected Health Information is not centrally located, each HIPAA Policy Group member shall provide (and shall update as necessary) the Privacy Contact with (i) the location of all Protected Health Information and (ii) a copy of the key, the password or any other device or means necessary to access the Protected Health Information.

Documentation. In the event a HIPAA Policy Group member makes a disclosure under this HIPAA Policy requiring documentation, see the Documenting Disclosures and Accountings Policy in Part 2 of this HIPAA Policy, HIPAA Authorized Employees member shall document such disclosure pursuant to the Record Retention and Documentation Policy.

Implementation. Each HIPAA Policy Group member shall implement any and all changes to this HIPAA Policy as directed by the Privacy Contact.

FORMS AND NOTICES

Authorization For Use of Disclosure Of Health Information

TOWN OF WEST BOYLSTON MASSACHUSETTS

AUTHORIZATION

I, _____, hereby authorize the use or disclosure of my health information as described in this authorization.

The following items MUST be completed by the employee or his duly authorized representative:

1. Name person/organization (or class of persons) authorized to provide the health information:

   _____

2. Name person(s)/organization(s) (or class of person) authorized to receive and use the information:

   _____

3. Provide a specific and meaningful description of the information you authorize to be disclosed (*Example:* "medical examination report and conclusions related to a fitness-for-work exam" or "results of drug testing for employment"):

   _____

   _____

   _____

   NOTE: If this authorization relates to a use or disclosure of psychotherapy notes, it may not be combined with an authorization to disclose any other health information.

4. State the purpose of the request (If you do not wish to state a purpose, please state, "at the request of the individual."):

   _____

   _____

The following paragraphs describe your rights with respect to this Authorization:

1. I understand that I have the right to revoke this authorization at any time by notifying in writing the person/organization authorized herein at (address of covered entity). I understand that the revocation is only effective after it is received and logged by such person/organization. I understand that any use or disclosure made prior to the revocation of the authorization will not be affected by the revocation nor will the revocation apply to disclosures made in reliance on this authorization.

2. I understand that after this information is disclosed, federal or state law might not protect it and the recipient might redisclose it.

3. [**If the authorization is NOT for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations, insert the following:]**

   I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment or payment or my eligibility for benefits.

   [If the authorization is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations, you may insert the following:]

   I understand that I may refuse to sign this authorization; however, if I do not sign the authorization, the Health Plan may refuse to enroll me.

4. I understand that my initial and continued employment and position are subject to my agreement to this authorization, and any additional authorization Town of West Boylston requests.

   [If applicable and to the extent consistent with employment handbooks and any applicable collective bargaining or state-law restrictions (imposed either voluntarily or by law.)]

5. I understand that I am entitled to receive a copy of this authorization.

6. I understand: (*Please check one)*

☐ this authorization will expire when my employment with the Town of West Boylston terminates.

☐ this authorization will terminate once the purpose for the authorization has been accomplished.

☐ this authorization will terminate on _____(*insert date*) or sooner in the event I revoke the authorization in writing as provided above.

☐ this authorization will terminate upon (*describe event*):

_____

_____

[The authorization must include a terminal date based on a specific date or event.]

Signature of Employee _____

Date _____

Personal Representative's Section:

I, _____, hereby certify that I am the personal representative of _____ and warrant that I have the authority to sign this form on the basis of:

_____

_____

Sample Business Associate Contract Provisions

HIPAA Privacy Confidentiality Agreement

TOWN OF WEST BOYLSTON, MASSACHUSETTS

HIPAA PRIVACY CONFIDENTIALITY AGREEMENT

Effective _____, 20__

I, _____, have read and agree to comply with the Town of West Boylston HIPAA Policy ("HIPAA Policy") regarding the privacy of Individually Identifiable Health Information (or "Protected Health Information"), as mandated by the Health Insurance Portability and Accountability Act of 1996 (the "HIPAA Privacy Rule"), as amended, and applicable state law.

I acknowledge that I have received training in such policies concerning Protected Health Information use, disclosure, storage and destruction.

In consideration of my employment or compensation from the Town of West Boylston, I hereby agree that:

- I will not at any time - either during my employment or association with Town of West Boylston Prior after my employment or association ends - use, access or disclose Protected Health Information to any person or entity, internally or externally, except as is required and permitted in the course and scope of the duties of the position to which I have been assigned, as set forth in the HIPAA Policy or as permitted under the HIPAA Privacy Rule.
- This obligation extends to any Protected Health Information that I may acquire during the course of my employment or association with Town of West Boylston, Massachusetts, whether in oral, written, electronic or any other form and regardless of the manner in which access was obtained.
- I will comply with the requirements of the HIPAA Policy during the course of my employment or association.
- Unauthorized uses or disclosures of Protected Health Information may result in disciplinary action, up to and including the termination of my employment or association

with the Town of West Boylston. Civil or criminal penalties under applicable federal and state law, as well as professional disciplinary action, may also apply.

- The terms of this agreement and my obligations hereunder shall survive the termination of my employment or end of my association with Town of West Boylston, Massachusetts, regardless of the reason for such termination.

Signed Date

_____ _____

Protected Health Information Disclosure Log

(COVERED ENTITY)

PROTECTED HEALTH INFORMATION DISCLOSURE LOG

Individual's name: _____ Date of birth_____

Dates Covered by this Accounting Sheet: **_____ to _____**

The individual has the right to an accounting of disclosures made up to six (6) years prior to the date of the request

Date	Protected Health Information disclosed	To Whom Disclosed Name/Address	Basis for Disclosure	For multiple disclosures to single person/entity for single purpose, frequency, and date of last disclosure for accounting period.

Notice of Privacy Practices For Protected Health Information

TOWN OF WEST BOYLSTON, MASSACHUSETTS

NOTICE OF PRIVACY PRACTICES

The privacy practices described in this notice apply to the Town of West Boylston's Group Health Plan and (list other plans such as FSA HRS etc.)t sponsored by Town of West Boylston, Massachusetts (the "Plan"). The Plan is required by the federal law known as the Health Insurance Portability and Accountability Act (referred to as the HIPAA Privacy Rule) to make reasonable steps to ensure the privacy of your personally identifiable health information (*Protected Health Information*) and to inform you about:

- your Plan's uses and disclosures of *Protected Health Information*;
- your privacy rights with respect to your *Protected Health Information*;
- your right to file a complaint with your Plan and to the Secretary of the U.S. Department of Health and Human Services; and
- the person or office to contact for further information about your Plan's privacy practices.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Except as otherwise described in this notice or otherwise permitted under the HIPAA Privacy Rule, uses and disclosures of *Protected Health Information* will be made only with your written authorization subject to your right to revoke such authorization.

USES AND DISCLOSURES TO CARRY OUT TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

The HIPAA Privacy Rule permits the Plan and its respective Business Associates to use *Protected Health Information* without your consent, authorization, or opportunity to agree or object, to carry out Treatment, Payment and Health Care Operations.

- *Treatment* refers to the provision and coordination of health care by a doctor, hospital or other health care provider. As a group health plan and/or group medical FSA we do not provide treatment.

- *Payment* includes but is not limited to actions to make coverage determinations and payment (including billing, claims management, subrogation, plan reimbursement, reviews for medical necessity and appropriateness of care and utilization review and preauthorizations). For example, PHI may be used in the billing, collection and payment of premiums and fees to plan vendors, utilization review companies, prescription drug card companies and reinsurance carriers; or PHI may be disclosed to an external medical review company to determine the medical necessity or experimental status of a treatment.

- *Health Care Operations* include but are not limited to quality assessment and improvement, reviewing competence or qualifications of health care professionals, underwriting, premium rating and other insurance activities relating to creating or renewing insurance contracts. For example, the Plan may use information about your claims to refer you to a disease management program, project future benefit costs or audit the accuracy of its claims processing functions.

USES AND DISCLOSURES THAT REQUIRE YOUR WRITTEN AUTHORIZATION

Your written authorization is generally required before the Plan will use or disclose psychotherapy notes about you from your psychotherapist. Psychotherapy notes are separately filed notes about your conversations with your mental health professional during a counseling session. They do not include summary information about your mental health treatment. The Plan may use and disclose such notes when needed by the Plan to defend against litigation filed by you.

USES AND DISCLOSURES THAT REQUIRE THAT YOU BE GIVEN AN OPPORTUNITY TO AGREE OR DISAGREE PRIOR TO THE USE OR RELEASE

Disclosure of your *Protected Health Information* to family members, other relatives and your close personal friends is allowed if:

- the information is directly relevant to the family or friend's involvement with your care or payment for that care; and

- you have either agreed to the disclosure or have been given an opportunity to object and have not objected.

USES AND DISCLOSURES FOR WHICH CONSENT, AUTHORIZATION OR OPPORTUNITY TO OBJECT IS NOT REQUIRED

Use and disclosure of your *Protected Health Information* is allowed without your consent, authorization or request under the following circumstances:

- When required by law.
- When permitted for purposes of public health activities, including if you have been exposed to a communicable disease or are at risk of spreading a disease or condition, if authorized by law.
- When authorized by law to report information about certain abuse, neglect or domestic violence to public authorities.
- For public health oversight activities authorized by law.
- For certain judicial or administrative proceedings.
- For certain law enforcement purposes
- To a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death or other duties as authorized by law; and funeral directors, consistent with applicable law.
- The Plan may use or disclose *Protected Health Information* for research, subject to conditions.
- For the purpose of facilitating organ, eye or tissue donation or transplantation.
- When consistent with applicable law to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.
- To the extent necessary to comply with workers' compensation or other similar programs established by law.
- Disclosures to Legal Counsel as part of the Town of West Boylston's litigation and litigation avoidance policy including accident reporting.

REQUIRED USES AND DISCLOSURES

Upon your request, your Plan is required to give you access to certain *Protected Health Information* in order to inspect and copy it. Under certain circumstances, however, the Plan may deny your request.

Use and disclosure of your *Protected Health Information* may be required by the Secretary of the Department of Health and Human Services to investigate or determine the Plan's compliance with the privacy regulations.

RIGHTS OF INDIVIDUALS

In the event any of the following rights require you to submit a written request to exercise such right, you must submit such request to the HIPAA Privacy Contact, 325 Main Street, West Boylston, MA 01540.

RIGHT TO REQUEST RESTRICTIONS OF PROTECTED HEALTH INFORMATION USES AND DISCLOSURES

You may request that your Plan restrict uses and disclosures of your *Protected Health Information* to carry out Treatment, Payment or Health Care Operations, or to restrict uses and disclosures to persons identified by you who are involved in your care or payment for your care. However, the Plan is not required to agree to your request.

Your Plan will accommodate reasonable requests to receive communications of *Protected Health Information* by alternative means or at alternative locations. You or your personal representative will be required to complete a form to request restrictions on uses and disclosures of your *Protected Health Information*.

RIGHT TO INSPECT AND COPY PROTECTED HEALTH INFORMATION

You have a right to inspect and obtain a copy of your *Protected Health Information* contained in a "Designated Record Set," for as long as your Plan maintains the *Protected Health Information*.

- "Designated Record Set" includes enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for a health plan, or other information used in whole or in part by or for the Covered Entity to make decisions about individuals. Information used for quality control or peer review analyses and not used to make decisions about individuals is not in the Designated Record Set.

The requested information will be provided within 30 days for on-site information and within 60 days for off-site information. A single 30-day extension is allowed if your Plan or its Business Associates are unable to comply with the deadline. Your Plan will charge a reasonable, cost-based fee to cover the cost of providing copies.

You or your personal representative will be required to complete a form to request access to the *Protected Health Information* in your Designated Record Set. If access is denied, you or your personal representative will be provided with a written denial setting forth the basis for the denial, a description of how you may exercise those review rights and a description of how you may complain to the Secretary of the U.S. Department of Health and Human Services.

RIGHT TO AMEND PROTECTED HEALTH INFORMATION

You have the right to request your Plan to amend your *Protected Health Information* or a record about you in a Designated Record Set for as long as the *Protected Health Information* is maintained in the Designated Record Set.

The Plan has 60 days after the request is made to act on the request. A single 30-day extension is allowed. If the request is denied in whole or part, your Plan must provide you with a written denial that explains the basis for the denial. You or your personal representative may then submit a written statement disagreeing with the denial and have that statement included with any future disclosures of your *Protected Health Information*.

You or your personal representative will be required to complete a form to request amendment of the *Protected Health Information* in your Designated Record Set. Any request for an amendment must be in writing and provide a reason to support a requested amendment.

THE RIGHT TO RECEIVE AN ACCOUNTING OF PROTECTED HEALTH INFORMATION DISCLOSURES

Upon your written request, your Plan will also provide you with an accounting of disclosures by the Plan of your *Protected Health Information* during the six years prior to the date of your request. However, such accounting need not include *Protected Health Information* disclosures made: (1) to carry out

Treatment, Payment or Health Care Operations; (2) to individuals about their own *Protected Health Information*; (3) prior to the compliance date; or (4) based on your written authorization.

If the accounting cannot be provided within 60 days, an additional 30 days is allowed if the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided. If you request more than one accounting within a 12-month period, your Plan will charge a reasonable, cost-based fee for each subsequent accounting.

A NOTE ABOUT PERSONAL REPRESENTATIVES

You may exercise your rights through a personal representative. Your personal representative will be required to produce evidence of his/her authority to act on your behalf before that person will be given access to your *Protected Health Information* or allowed to take any action for you.

Your Plan retains discretion to deny access to your *Protected Health Information* to a personal representative to provide protection to those vulnerable people who depend on others to exercise their rights under these rules and who may be subject to abuse or neglect.

YOUR PLAN'S DUTIES

Your Plan is required by law to maintain the privacy of *Protected Health Information* and to provide participants and beneficiaries with notice of its legal duties and privacy practices. The Town will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.

This notice is effective beginning (Date) and the Plan is required to comply with the terms of this notice. However, the Plan reserves the right to change its privacy practices and to apply the changes to any *Protected Health Information* received or maintained by the Plan prior to that date.

If a privacy practice is changed, a revised version of this notice will be provided to all past and present participants and beneficiaries for whom the Plan still maintains *Protected Health Information*. The revised notice in the preceding sentence shall be provided by first class mail to a participant or beneficiary's last known address. Any revised version of this notice will be distributed within 60 days of the effective date of any material change to the uses or disclosures, the individual's rights, the duties of your Plan or other privacy practices stated in this notice.

MINIMUM NECESSARY STANDARD

When using or disclosing *Protected Health Information* or when requesting *Protected Health Information* from another Covered Entity, the Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of *Protected Health Information* necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations. However, the minimum necessary standard will not apply in the following situations:

- disclosures to or requests by a health care provider for treatment;
- uses or disclosures made to the individual or pursuant to your authorization;
- disclosures made to the Secretary of the U.S. Department of Health and Human Services;
- uses or disclosures that are required by law; and
- uses or disclosures that are required for the Plan's compliance with legal regulations.

In addition, your Plan may use or disclose enrollment information to the (covered entity) as well as "summary health information" for obtaining premium bids or modifying, amending or terminating the Plan, which summarizes the claims history, claims expenses or type of claims experienced by individuals for whom a member of Town of West Boylston, Massachusetts has provided health benefits under the Plan, and from which identifying information has been deleted in accordance with HIPAA. Your Plan may also disclose *Protected Health Information* to the Town of West Boylston, Massachusetts for treatment, payment or health care operations as permitted under HIPAA.

YOUR RIGHT TO FILE A COMPLAINT WITH THE PLAN OR THE HHS SECRETARY

If you believe that your privacy rights have been violated, you may file a written complaint with the Plan in care of the following contact: (name, title and work address of HIPAA officer)

or

you may file a complaint with the Secretary of the U.S. Department of Health and Human Services, Hubert H. Humphrey Building, 200 Independence Avenue S.W., Washington, D.C. 20201. Your Plan will not retaliate against you for filing a complaint.

ADDITIONAL INFORMATION

If you have any questions regarding this notice or the subjects addressed in it, you may contact the Plan Privacy Contact, (Name Address and phone number)

The HIPAA Privacy Rule is set out at 45 Code of Federal Regulations Parts 160 and 164. These regulations and additional information about 45 CFR Parts 160 and 164 et seq. are available at http://www.hhs.gov/ocr/hipaa/.

Request For Access to Protected Health Information

TOWN OF WEST BOYLSTON, MASSACHUSETTS

REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

I, _____, hereby request that the group health plan sponsored by Town of West Boylston ("Plan") permit me to access my health information described below and in the following manner:

This request related to the following health information:

_____

_____

_____

_____

Please check one of the items below:

- ❑ I would like the Plan to permit me or my duly appointed representative access to the health information described above for inspection.

- ❑ I would like the Plan to provide me or my duly appointed representative with copies of the health information described above. ***By making this request, I agree to reimburse the Plan for any and all costs it incurs in providing the copies requested.***

I understand that under some circumstances the Plan is permitted to deny my request.

I understand that the Plan will generally respond to my request within 10 days after it receive this request. If, however, the health information described above is only maintained or accessible to the Plan off-site, I understand that the Plan will have 60 days following the receipt of this request to respond. In addition,

in the event the Plan is unable to respond with the timeframes mentioned above, I understand that the time for responding may be extended for one time for no longer than 30 days.

Signature: _____ Date: _____

Request To Amend Protected Health Information

COVERED ENTITY)

REQUEST TO AMEND PROTECTED HEALTH INFORMATION

I, _____, hereby request that the group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") amend the Protected Health Information in its Designated Record Set.

Specifically describe the amendment requested:

_____

_____

_____

_____

Specifically describe the reason for the amendment requested:

_____

_____

_____

_____

I understand that under some circumstances the Plan is permitted to deny my request. For example, I understand that the Plan is not required to honor my request if the Protected Health Information: (i) was not created by the Plan; (ii) is not part of the Designated Record Set; (iii) would not be available to me to access; or (iv) is accurate and complete.

I understand that the Plan will generally respond to my request within 60 days after it receives this request. If, however, the Plan is unable to respond with the timeframe mentioned above, I understand that the time for responding may be extended for one time for no longer than 30 days.

Signature: _____ Date: _____

Complaint Form

COVERED ENTITY

COMPLAINT FORM

I, _____, hereby submit the following complaint to the group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") regarding its HIPAA Policy.

Specifically describe your complaint:

I attest under penalties of perjury that the above complaint is true and correct to the best of my knowledge.

Signature: _____ Date: _____

Request For Confidential Communications Of Protected Health Information

TOWN OF WEST BOYLSTON, MASSACHUSETTS

REQUEST FOR CONFIDENTIAL COMMUNICATIONS OF PROTECTED HEALTH INFORMATION

I, _____, hereby request that the group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") communicate Protected Health Information to me through the following alternative means and/or at the following alternative locations:

Specify the alternative means requested:

_____

_____

_____

_____

Specify the alternative locations:

_____

_____

_____

_____

I understand that the Plan may deny this request if the Privacy Contact finds it to be unreasonable or finds that the Plan cannot accommodate the request. I understand that I will be notified in the event the Plan cannot accommodate this request.

I understand that the Plan may not require me to explain the basis for this request. I understand that the disclosure of all or part of the information to which this request pertains could put me in danger.

Signature: _____ Date: _____

Request For An Accounting Of Disclosures Of Protected Health Information

TOWN OF WEST BOYLSTON, MASSACHUSETTS

REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

I, _____, hereby request that the group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") provide an accounting of all the disclosures of my health information it has made for the period beginning on _____ and ending on _____.

I understand that this request may not relate to a disclosure of Protected Health Information made by the Plan more than 6 years before the date of this request.

Please check one of the items below:

- ❑ I understand that because this is my first request for an accounting of disclosures of my Protected Health Information in a 12-month period, the accounting shall be provided without charge.

- ❑ I understand that because I have already made one request for an accounting of disclosures of my Protected Health Information during this 12-month period, ***I agree to reimburse the Plan for any and all costs it incurs in providing the accounting requested.***

I understand that the Plan is not required to document certain disclosures and that as such those disclosures are not subject to this request. In addition, I understand that under certain circumstances my right to have an accounting of the disclosures of my Protected Health Information may be suspended by a health oversight committee or a law enforcement agency.

I understand that for disclosures the Plan must account for, the accounting shall provide:

- The date of the disclosure;

- The name and, if known, the address of the person to whom the disclosure was made;
- A brief description of the Protected Health Information which was disclosed; and
- A brief statement of the purpose for the disclosure that reasonably sets forth the basis upon which the disclosure was made.

I understand that the Plan will generally respond to my request within 60 days after it receive this request. In addition, in the event the Plan is unable to respond with the timeframe mentioned above, I understand that the time for responding may be extended one time for no longer than 30 days.

Signature: _____ Date: _____

Request For A Restriction on Protected Health Information

TOWN OF WEST BOYLSTON, MASSACHUSETTS

REQUEST FOR A RESTRICTION ON PROTECTED HEALTH INFORMATION

I, _____, hereby request that the group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") restrict access to my health information as described below:

Describe the Protected Health Information that is the subject of this request and the type of restrictions you would like placed on this information: (*Attach a separate if necessary.*)

_____

_____

_____

_____

I understand that the Plan is not required to agree to the restriction requested above. In addition, I understand that if I am in need of emergency treatment and the information that is the subject of this request is needed to provide such treatment, the Plan may disclose the information to a provider in order to provide the treatment, regardless of the restriction described above.

Signature: _____ Date: _____

Response to Employee's Request to Access Protected Health Information

[COVERED ENTITY]]

[LETTERHEAD]

[Date]

[Employee or Representative]

[Address]

RE: Request to Access Protected Health Information

Dear **[Employee or Representative]**:

[If the request seeks only access, response below is due within 30 days of request without extension or within 60 days of receipt in the event the Protected Health Information requested is not maintained or accessible on-site.]

The group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") has approved your request to access your health information. Accordingly, the Plan will provide access at **[state the manner in which access will be provided]**.

If you have any questions, please contact HIPAA Authorized Employees at **[telephone number]**.

[OR, If the request seeks copies of Protected Health Information, response below is due within 30 days of request without extension, or within 60 days of receipt in the event the Protected Health Information requested is not maintained or accessible on-site.]

The group health plan sponsored by (covered entity) ("Plan") has approved your request for copies of your health information and has enclosed the copies requested. 45 CFR Parts 160 and 164 et seq. entitles the Plan to be reimbursed for the cost of providing these copies to you. Accordingly, please forward to the address above a check made payable to "**[insert name]**" in the amount **[$x.xx]** to cover the cost of providing the copies.

If you have any questions, please contact HIPAA Authorized Employees at **[telephone number]**.

[OR: If Plan needs an extension of time to respond which must be provided within 30 days of the date the request was received, or within 60 days of receipt in the event the Protected Health Information requested is not maintained or accessible on-site.]

The group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") received your request for access to health information on _____. The Plan has evaluated your request, however, a delay in action is necessary because **[describe reason for the delay]**.

The Plan will respond to your request by _____. **[list date that is no later than 60 days from the date of the request, or within 90 days of receipt of the request in the event the Protected Health Information requested is not maintained or accessible on-site.]**.

If you have any questions, please contact HIPAA Authorized Employees at **[telephone number]**.

[OR: If Plan denies the request to access, and such denial is not subject to review, the denial must be provided within 30 days of the date the request was received, or within 60 days of receipt in the event the Protected Health Information requested is not maintained or accessible on-site.]

The group health plan sponsored by 9covered entity0 ("Plan") received your request to amend health information on _____. Your request is denied because **[state the basis for the denial]**.

[If the requestor is entitled to a review of the decision, include: (i) a statement that the employee may have the right to have a licensed health care professional, chosen by the Plan, review the denial; and (ii) a description of how the individual may exercise such review rights.]

You may file a complaint regarding this decision with the Plan or the U.S. Department of Health and Human Services. If you file a complaint with the Plan, please file it in writing with the following person: **[state the name or title and telephone number of the contact person designated to receive complaints]**.

If you have any questions, please contact HIPAA Authorized Employees at **[telephone number]**.

Response to Employee's Request to Amend Protected Health Information

[COVERED ENTITY]

[LETTERHEAD]

[Date]

[Employee or Representative]

[Address]

RE: Request to Amend Protected Health Information

Dear **[Employee or Representative]**:

[If Plan approves the request to amend which must be provided within 60 days of the date the request was received.]

The group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") has approved your request to amend or correct your health information. Accordingly, the Plan will make an appropriate amendment to the Designated Record Set.

You must provide the Plan with the names of any persons to whom you wish to provide the amended information. The Plan then will make reasonable efforts to inform these individuals, as well as any other individuals pursuant to its HIPAA Policy.

If you have any questions, please contact HIPAA Authorized Employees at **[telephone number]**.

[OR: If Plan needs an extension of time to respond which must be provided within 60 days of the date the request was received.]

The group health plan sponsored by (covered entity) ("Plan") received your request to amend health information on _____. The Plan has evaluated your request, however, a delay in action is necessary because **[describe reason for the delay]**.

The Plan will respond to your request by _____. **[list date that is no later than 90 days from the date of the request]**.

If you have any questions, please contact HIPAA Authorized Employees at **[telephone number]**.

[OR: If Plan denies the request to amend which must be provided within 60 days of the date the request was received.]

The group health plan sponsored by Town of West Boylston, Massachusetts ("Plan") received your request to amend health information on _____. Your request is denied because **[state the basis for the denial]**.

You have the right to file a written statement disagreeing with the denial of amendment. The statement of disagreement must be limited to two-single-sided 8-1/2 x 11 pages. [The length restriction may be established by the plan and must be reasonable.] **The statement of disagreement should be filed within 60 days of this notice with the following office** [list individual or office]**. The Plan has the right to prepare a rebuttal statement to your statement of disagreement. If it does so, you will receive a copy.**

If you do not submit a statement of disagreement, you may request that the Plan provide your request for amendment and this denial of amendment with any future disclosures of Protected Health Information that is the subject of this request. You may file a complaint regarding this decision with the Plan or the U.S. Department of Health and Human Services. If you file a complaint with the group health plan, please file it in writing with the following person: **[state the name or title and telephone number of the contact person designated to receive complaints]**.

If you have any questions, please contact HIPAA Authorized Employees at **[telephone number]**.