Office of the
BOARD OF SELECTMEN
272 Main Street
Townsend, Massachusetts 01469

Carolyn Smart, *Chairman* | Gordon Clark, *Vice-Chairman* | *Cindy King, Clerk*
James M Kreidler, Jr.
Town Administrator
Office (978) 597-1701
Fax (978) 597-1719

POLICY #1-2017
BOARD OF SELECTMEN

HIPAA PRIVACY POLICY
UPDATED: January, 2017

Introduction

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended, as well as its implementing regulations, restrict the Town's ability to use and disclose protected health information ("PHI"). PHI is defined as follows:

> information that is created or received by the Town and relates to the past, present, or future physical or mental health or condition of a patient; 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 for which there is a reasonable basis to believe the information can be used to identify the individual. Protected health information includes information of persons living or deceased.

It is the Town's policy to fully comply with HIPAA's requirements, including the Privacy Rule, Public Law 104-191 and the Health Information Technology for Economic and Clinical Health (HITECH) Act. To that end, all Town employees who have access to PHI must comply with this Privacy Policy. For purposes of this Policy and the Town's PHI use and disclosure procedures, the term "Town employee shall be defined to include all elected and appointed Town officials and all individuals who would be considered part of the workforce under HIPAA, including Town employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Town, whether or not they work on a full or part-time basis or are paid by the Town.

.

No third party rights are intended to be created by this Policy. The Town reserves the right to amend or change this Policy at any time without notice. This Policy is limited solely to the Town's privacy obligations under HIPAA, and does not address any other applicable requirements under other federal or state laws.

This Privacy Policy shall address the following:

- The Town's Privacy Official and Contact Persons;
- Town Employee Training;

- Technical and Physical Safeguards of PHI;
- Privacy Notice;
- Complaints;
- Sanctions for Violations of Privacy Policy;
- Mitigation of Inadvertent Disclosures of PHI;
- No Intimidating or Retaliatory Acts or Waiver of HIPAA Privacy;
- Disclosure of PHI;
- Documentation;
- The Use and Disclosure of PHI;
- Town Employees' Compliance with the Town's Privacy Policy and Procedures;
- Access to PHI;
- Permitted Uses and Disclosures;
- No Disclosure of PHI for Non-Authorized Reasons;
- Mandatory Disclosures of PHI
- Permissive Disclosures of PHI for Public Interest and Benefit Activities;
- Disclosures of PHI Pursuant to an Authorization;
- Complying with the "Minimum-Necessary" Standard;
- Disclosures of PHI to Business Associates;
- Disclosures of De-Identified Information;
- Access to PHI and Requests for Amendment;
- Accounting;
- Breach Notification;
- Requests for Restrictions on Uses and Disclosures of PHI; and
- Enforcement.

The Town's Responsibilities as Covered Entity

I. The Town's Privacy Official and Contact Person

James M. Kreidler, Jr. shall be the Privacy Official for the Town of Townsend. The Privacy Official can be reached at:

Address: 272 Main Street, Townsend, MA 01469
Telephone: 978-597-1701
Fax: 978-597-1719
E-Mail: jkreidler@townsend.ma.us

The Privacy Official shall be responsible for the development and implementation of policies and procedures relating to privacy of PHI, including but not limited to this Privacy Policy and the Town's PHI use and disclosure procedures. The Privacy Official shall also serve as the contact person for individuals who have questions, concerns, or complaints about the privacy of their PHI.

II. Town Employee Training

It is the Town's policy to train all members of its workforce who have access to PHI on HIPAA's privacy and security policies and procedures. The Privacy Official is charged with developing training schedules and programs so that all Town employees with access to PHI receive necessary and appropriate training to adhere to HIPAA's requirements.

III. Technical and Physical Safeguards of PHI

Pursuant to this Policy, the Town shall establish appropriate technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Appropriate technical safeguards for purposes of this policy shall include, but not be limited to, password protecting computers and documents, implementing electronic security measures and limiting access to electronic information by creating computer firewalls. Appropriate physical safeguards for purposes of this policy shall include, but not be limited to, appropriately securing areas in Town where PHI is stored.

Appropriate technical and physical safeguards shall be designed to ensure that only authorized Town employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

In furtherance of this Policy, the Town has adopted a HIPAA Security Policy to ensure compliance with HIPAA's Security Rule. 45 CFR 160, 162, and 164.

IV. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Town's privacy practices ("Notice of Privacy Practices") that describes:

- the uses and disclosures of PHI that may be made by the Town;
- individual rights; and
- the Town's legal duties with respect to the PHI.

The Notice of Privacy Practices shall inform individuals that the Town will have access to PHI in connection with its medical and administrative functions. In addition, the Notice of Privacy Practices will provide a description of the Town's complaint procedures, the name and telephone number of the designated Privacy Official, and the date of the notice.

To the extent practicable, the Notice of Privacy Practices shall be individually delivered to all persons receiving medical attention or otherwise providing the Town with PHI subject to the protections of HIPAA:

- On an ongoing basis, at the time of an individual's medical treatment and consent, or, if such time is not practicable, at the earliest possible time thereafter; and
- Within 60 days after a material change to the Notice of Privacy Practices.

The Notice of Privacy Practices shall also be posted in Town Hall, posted on the Town's website and made available upon request to the Town's Privacy Official.

V. Complaints

The Town's Privacy Official shall be the Town's contact persons for receiving complaints concerning use and disclosure of PHI. The Privacy Official shall be responsible for creating a process for receiving, investigating and addressing complaints lodged with regard to the Town's PHI privacy procedures.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy shall be imposed in accordance with the Town's policies and procedures, and, for Town employees, shall include the potential for termination.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

The Town shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in this Privacy Policy.

Pursuant to this Privacy Policy, if an employee becomes aware of the use or disclosure of PHI, either by a Town employee or an outside consultant/contractor, that is not in compliance with this Privacy Policy, the employee shall immediately contact a Privacy Official so that the appropriate steps to mitigate the potential harm, including, but not limited to, notification of a potential breach to the individual(s) affected and to the U.S. Department of Health and Human Services ("HHS") Secretary, as set forth in the Breach Notification section of this Policy.

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

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

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

IX. Disclosure of PHI

Pursuant to this Policy, the Town, its officials and employees, shall adhere to the following disclosure guidelines:

- PHI shall be used or disclosed only as authorized and/or required by law;
- Ensure that any agents or subcontractors that will receive PHI from the Town agree prior thereto to comply with the same restrictions and conditions that apply to the Town concerning use or disclosure of PHI by executing a Business Associate Agreement;
- PHI shall not be disclosed for employment-related actions;
- Report immediately or as soon as practicable to a Privacy Official any use or disclosure of PHI that is inconsistent with the permitted uses or disclosures authorized by law and this Privacy Policy; and
- Make the Town's internal practices and records relating to the use and disclosure of PHI received available to the Department of Health and Human Services upon request.

X. Documentation

The Town's privacy policies and procedures shall be documented and maintained for at least six years and otherwise as required by the state law. Policies and procedures shall be amended from time to time as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications to the applicable regulations). Any changes to policies or procedures shall be promptly documented.

Upon the effective date of this Policy, the Town shall document events and actions relating to an individual's privacy rights under HIPAA, including authorizations for use or disclosure, requests for information concerning use or disclosure of PHI, complaints concerning use or disclosure of PHI, and any sanctions imposed as a result of misuse or improper disclosure.

The documentation of any policies and procedures, actions, activities and designations shall, to the extent permitted by law, be maintained in either written or electronic form for at least six years, and otherwise as required by state law.

Policies on the Use and Disclosure of PHI

I. Use and Disclosure Defined

The Town shall use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the benefits area of the Town, or by a Business Associate of the Town.

- *Disclosure.* For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not authorized by the Town to have access to PHI.

II. Workforce Must Comply With Town's Privacy Policy and Procedures

All Town employees who have access to PHI shall comply with this Privacy Policy, as well as with any procedures promulgated hereunder.

III. Access to PHI Is Limited to Certain Employees

Town employees with access to PHI shall not disclose PHI to employees (other than to employees with authorized access) unless an authorization has been provided or the disclosure otherwise is in compliance with this Policy.

IV. Permitted Uses and Disclosures

The Town, as a so-called "covered entity" for purposes of HIPAA, is permitted, but not required, to use and disclose PHI, without an individual's authorization, for the following purposes or situations: (1) to the individual (unless required for access or accounting of disclosures); (2) for treatment, payment, and health care operations; (3) to the individual after the individual has had an opportunity to agree or object to the use and disclosure of the PHI; (4) incident to an otherwise permitted use and disclosure; (5) public interest and benefit activities; and (6) limited data set for the purposes of research, public health or health care operations.

- *Treatment.* Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

- *Payment.* Payment includes activities undertaken to obtain an individual's contributions or to determine or fulfill the Town's responsibility for provision of

benefits subsequent to providing medical services, or to obtain or provide reimbursement for health care. Payment also includes:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics; and
- billing, claims management, collection activities and related health care processing.

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

- *Health Care Operations.* Health care operations mean any of the following activities to the extent that they are related to the Town's emergency medical care administration:
  - conducting quality assessment and improvement activities;
  - reviewing health care performance;
  - conducting or arranging for medical review, legal services and auditing functions;
  - planning and development; and
  - business management and general administrative activities.

V. No Disclosure of PHI for Non-Authorized Reasons

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's PHI may be used or disclosed by covered entities. Therefore, neither the Town nor any Town employee shall use or disclose PHI, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

VI. Disclosures of PHI

An individual's PHI shall be disclosed under HIPAA if:

1. The disclosure is to the individual who is the subject of the information;
2. The disclosure is to friends and family members involved in your care of payment of your care, unless we determine disclosure is not in an individuals' best interest; and
3. The disclosure is made to the U.S. Department of Health and Human Services for purposes of enforcing HIPAA.

VII. Permissive Disclosures of PHI: for Public Interest and Benefit Activities

The Town may disclose PHI in the following situations without an individual's authorization, for so-called "national priority" purposes as that term is used in HIPAA. These disclosures are permitted, although not required, by the Privacy Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, as set forth in HIPAA, striking the balance between the individual privacy interest and the public interest need for the information. Prior to disclosure for such purposes, a Town employee shall review with the Privacy Official whether potential uses or disclosures are authorized for any of the below reasons.

- Required by law;
- Public health activities;
- Victims of abuse, neglect or domestic violence;
- Health oversight activities;
- Judicial and administrative proceedings;
- Certain law enforcement purposes;
- Decedents;
- Cadaveric organ, eye or tissue donation;
- Research;
- Serious threat to health or safety;
- Essential government functions; and
- Workers' Compensation.

VIII. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose, including marketing purposes, if an individual executes an authorization that satisfies all of HIPAA's requirements. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

IX. Complying With the "Minimum-Necessary" Standard

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

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

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;

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

Minimum Necessary When Disclosing PHI. For making disclosures of PHI to any Business Associate or for claims payment/adjudication, design and pricing or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.
All other disclosures shall be reviewed on a case by case basis with the designated Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.
Minimum Necessary When Requesting PHI. When a Town employee *requests* disclosure of PHI by Business Associates, providers or individuals for purposes of claims payment/adjudication, design and pricing or internal/external auditing purposes, only the minimum necessary amount of information shall be requested.
All other requests shall be reviewed on an individual basis with the designated Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

X. Disclosures of PHI to Business Associates

Authorized Town employees may disclose PHI to the Town's business associates and allow the Town's business associates to create or receive PHI on its behalf. Prior to creating or receiving PHI, the Town must first obtain written assurances from the business associate(s) that it will appropriately safeguard the information.

Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," Town employees shall contact the designated Privacy Official and verify that a business associate contract is currently in effect.

A Business Associate is an entity that:

- performs or assists in performing a Town function or activity involving the use and disclosure of PHI (including claims processing or administration, data analysis, underwriting, etc.); or
- provides medical, accounting, actuarial, consulting, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

XI. Disclosures of De-Identified Information

The Town may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing specific identifiers.

Policies on Individual Rights

I. Access to Protected Health Information and Requests for Amendment

This Privacy Policy acknowledges that HIPAA gives individuals the right to access and obtain copies of their PHI that the Town or its business associates maintains in designated record sets. There shall be restricted disclosures of documents that contain a patients' PHI to his/her health plan(s) if the patient has paid the out-of-pocket amount in full.

The Privacy Rule gives individuals the right to have covered entities amend their PHI in a designated record set when that information is inaccurate or incomplete. If the Town accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment. If the request is denied, the Town must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Rule specifies processes for requesting and responding to a request for amendment. The Town shall amend PHI in its designated record set upon receipt of notice to amend from another covered entity.

Except in certain circumstances, individuals have the right to review and obtain a copy of their PHI in the Town's designated record set. The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.

II. Accounting

Individuals have a right to an accounting of the disclosures of their PHI by the Town or the Town's business associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request, except that the Town shall not be obligated to account for any disclosure made before its Privacy Rule compliance date.

The Privacy Rule does not require accounting for disclosures: (a) for treatment, payment, or health care operations; (b) to the individual or the individual's personal representative; (c) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (d) pursuant to an authorization; (e) of a limited data set; (f) for national security or intelligence purposes; (g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (h) incident to otherwise permitted or required uses or disclosures.

Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.

III. Breach Notification Procedures

The Town shall provide notice as required under HIPAA when there is a breach of unsecured PHI in a manner not permitted under HIPAA. HIPAA requires that the Town notify individuals whose unsecured PHI has been compromised by such a breach. In certain circumstances, the Town must also report such breaches to the Secretary of HHS and through the media. The Town's breach notification process will be carried out in compliance with the Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009 and its implementing rules and regulations, each as may be

amended from time to time, including those regulatory amendments of the Department of Health and Human Services published at 78 Fed. Reg. 5566 (Jan. 25, 2013), collectively HIPAA.

Breach. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA, which compromises the security or privacy of the PHI. Breach excludes:

- Any unintentional acquisition, access, or use of PHI by a Town employee or person acting under the authority of the Town or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA.

- Any inadvertent disclosure by a person who is authorized to access PHI at the Town or business associate to another person authorized to access PHI at the Town or same business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

- A disclosure of PHI where the Town or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Discovery of Breach. A breach shall be treated as discovered as of the first day on which such breach is known to the Town or, by exercising reasonable diligence, would have been known to the Town or Town employee, other than the person committing the breach. Town employees who believe that an individual's information has been used or disclosed in any way that compromises the security or privacy of that information shall immediately notify a Town Privacy Official. Following the discovery of a potential breach, the Town shall immediately begin an investigation, conduct a risk assessment, and, based on the results of the risk assessment, begin the process of notifying each individual whose PHI has been, or is reasonably believed by the Town to have been, accessed, acquired, used, or disclosed as a result of the breach. The Town shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of the Department of Health and Human Services (HHS), media outlets, or law enforcement officials.

Breach Investigation. The Town's Privacy Official shall investigate the breach and shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others in the Town as appropriate (e.g., administration, police department, human resources, and legal counsel). The Town's entire workforce is expected to assist the Privacy Official in this investigation as requested. The Privacy Official shall be the key facilitators for all breach notification processes.

Notification: Individuals Affected. If it is determined that breach notification must be sent, a breach notification letter shall be sent out to all affected individuals. Notice to affected individuals shall contain the following information relevant information containing the breach, including a description of what happened, the type(s) of unsecured PHI that was involved in the breach, any appropriate steps that should be taken, relevant contact information and steps that the Town has taken to investigate the breach and mitigate any potential harm. Notice to affected individuals shall be made in accordance with HIPAA's requirements and without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If the Town determines that notification requires urgency because of possible imminent misuse

of unsecured PHI, notification may be provided by telephone or other means, as appropriate, in addition to the methods noted above. It is the responsibility of the Practice to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

Notification: HHS. In the event a breach of unsecured PHI affects 500 or more of the individuals, the Town will notify HHS at the same time notice is made to the affected individuals, in the matter specified on the HHS website. If fewer than 500 individuals are affected, the Town will maintain a log of the breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year, in the manner specific on the HHS website. The submission shall include all breaches discovered during the preceding calendar year.

Notification: Media. In the event the breach affects more than 500 residents of Massachusetts, prominent media outlets serving the state and regional area will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.

Business Associate Responsibilities. The Town's business associates shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach of unsecured PHI, notify the Town's Privacy Official of such breach. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. Upon notification by the business associate of discovery of a breach, the business associate, in consultation with the Town, will be responsible for notifying affected individuals and all costs associated with such notification, unless otherwise agreed upon in writing by the Town and the business associate.

IV. Requests for Restrictions on Uses and Disclosures of Protected Health Information

- **Restriction Request.** Individuals have the right to request that a covered entity restrict use or disclosure of PHI for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. The Town is under no obligation to agree to requests for restrictions. If the Town does agree, it must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

- **Confidential Communications Requirements.** The Town shall permit individuals to request an alternative means or location for receiving communications of PHI by means other than those that the Town typically employs. For example, an individual may request that the Town communicate with the individual through a designated address or phone number. Similarly, an individual may request that the provider send communications in a closed envelope rather than a post card. The Town may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

V. Enforcement

- Every Town employee with access to PHI is required to adhere to all HIPAA mandates.

- Violation of this Policy may result in disciplinary action up to and including termination of employment or other relationship with the Town in a full or part-time or volunteer capacity.
- Under state and federal law, violation of this Policy may result in significant civil monetary penalties as well as criminal sanctions, including, fines and imprisonment.

552064/TOWN/0001

ADOPTED BY THE BOARD OF SELECTMEN ON January 24, 2017

Carolyn Smart, Chairman

Gordon Clark, Vice-Chair

Cindy King, Clerk