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 #2-2017
BOARD OF SELECTMEN

HIPAA SECURITY POLICY

The Health Insurance Portability and Accountability Act ("HIPAA") Security Rule ("Security Rule"), 45 CFR 160, 162, and 164, regulates the administrative, technical and physical safeguards of Protected Health Information ("PHI"). The Security Rule regulates the protection of PHI data from unauthorized access, whether external or internal, stored or in transit.

To fully comply with the Security Rule's requirements, the Town of Townsend ("Town") has adopted the following Security Policy to comply with HIPAA and its amendments, including, but not limited to the Health Information Technology for Economic and Clinical Health (HITECH) Act. 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. This Policy sets forth the framework for the Town's compliance with the Security Rule.

I. Purpose

The Security Rule defines the standards, which require covered entities, such as the Town, to implement basic safeguards to protect the confidentiality and integrity of PHI. This Security Policy is implemented in compliance with the Security Rule.

II. Definitions

- Protected Health Information: 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.

- HIPAA Privacy Rule: regulates the use and disclosure of individuals' health

information—called "protected health information" by organizations subject to the Privacy Rule called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. The U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

- HIPAA Security Official: The Town's HIPAA Security official is the James M Kreidler,Jr..

- HIPAA Security Rule: The Security Rule establishes national standards for the security of electronic health care information. The Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of protected health information.

III. Requirements and Responsibilities

Under the Security Rule, the Town shall implement appropriate administrative, physical and technical safeguards to protect the integrity, confidentiality and availability of PHI that is created, received, managed or transmitted by the Town. The HIPAA Security Official may, at his/her discretion, implement appropriate safeguards and procedures in furtherance of this Security Policy.

A. Administrative Safeguards

1. Security Awareness and Training

    - All Town employees who are authorized to view, send, receive or manage PHI shall undergo HIPAA training.

    - To the extent necessary, Town employees who are authorized to view, send or receive PHI shall receive periodic security updates.

2. Workforce Security

    - Only authorized Town employees shall have access to records and systems that manage, view, store, send or receive PHI.

    - The Town shall, at its discretion, limit authorized personnel's access to PHI to the extent that access to this information achieves the requirements of the person's employment responsibilities.

    - The Town shall implement procedures for immediately terminating an authorized Town employee's access to PHI when the individual's employment terminates or when the employment responsibilities of the person no longer require that individual to access PHI.

    - The Town shall review its record systems in place to ensure that only currently authorized personnel have access to systems containing PHI.

3. Information Access Management

- Only authorized personnel shall have access to systems that contain, manage, view, store, send and/or receive PHI.

4. Password Management

- Town employees with access to PHI shall, at all times, maintain secure password management of their computers, smartphones, external hard drives, zip drives, servers, networks, and, if applicable, documents. In furtherance of this Policy, employees should choose a password that is difficult to guess and uses between six and eight unique characters.

- Passwords shall be regularly changed.

- Town employees shall, at all times, keep their passwords secure and private. Employees shall not share or authorize another Town employee to login to their computer, smartphones, external hard drives, zip drives, servers, and/or documents or network using his/her password.

- In the event that a Town employee believes that his/her password has been compromised, the employee shall immediately report the incident to the Security Official and change their login password immediately.

B. Physical Safeguards

1. Facility Access Controls

- The Town shall ensure that systems that send, store, maintain, manage or receive PHI are kept in secure areas with physical security controls in places which appropriately restrict access.

2. Workstation Use and Security

- Workstations, including filing cabinets and desk drawers, which contain PHI shall be secured at all times.

- All offices of Town facility areas which contain PHI shall remain secure at all times.

- Access to PHI secure areas, including workstations, filing areas and desks shall be limited at all times to HIPAA authorized personnel who have received HIPAA training.

- Under this Policy, only designated workstations with appropriate security controls shall be allowed to access and manage PHI.

- Workstations located in publicly accessible areas or used by multiple

users shall not be authorized to store or access PHI.

3. Record Retention/Disposal

- Under the Privacy Rule, the Town shall maintain, to the extent permitted by law, HIPAA policies and procedures, actions, activities and designations made by the Town in either written or electronic form for at least six years, and for such addition period as may be required by state law.

- Medical records shall be maintained in accordance with state law.

- The Town shall apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other documents that contain PHI for whatever period such information is maintained by a covered entity, including through disposal.

- The Town, consistent with state law, shall use proper disposal methods for medical records and other PHI which may include, but are not limited to:
  - For PHI in paper records, shredding, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed;
  - For PHI on electronic media, clearing (using appropriate software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, incinerating or shredding).

C. **Technical Safeguards**

1. Access Control

- All Town electronic devices, which send, receive, manage or maintain PHI shall comply with the Town's HIPAA policies.

2. Password Protection

- When a Town employee with access to PHI is away from his/her computer for more than five (5) minutes, the computer shall be secured with a password protected return from sleep or screen saver feature.

- No Town computer that contains access to PHI shall remain logged on outside of an employee's office hours or when the work station is vacated.

- Laptops, handheld PDA's, smartphones and cell phones, which contain PHI shall be locked and/or secured at all times and should

not be accessible without password entry.

- Laptops, handheld devices, storage media (backup drives, CDs, DVDs, zip drives or external hard drives) shall not be left unattended, should be fully secured and must remain password protected at all times.

- In the event that a Town owned laptop or other portable electronic device, including backup drives, which contain PHI is removed from Town property, the device shall maintain password protected at all times and be logged in and out with the Security Officer.

3. Transmission Security

- PHI shall only be transmitted using approved secure electronic messaging, including encryption and a secure transmission line.

- All attachments transmitting PHI electronically shall be password protected and encrypted.

- Prior to sending an electronic transmission of PHI, addresses of all recipients shall be carefully verified to avoid communication misdirection.

- Personal e-mail accounts (e.g. Gmail, Comcast, AOL, Yahoo, Hotmail) shall never be used to conduct Town business, including the transmission of messages or attachments, which contain PHI.

- If a Town employee believes that sensitive data has been compromised in any manner, the employee shall immediately notify the Town's Security Officer.

D. Town Employee Responsibilities

- Town employees shall abide by all applicable policies, including the Town's HIPAA Privacy Policy and Security Policy, to maintain the security and integrity of information systems and PHI.

- Town employees are responsible for notifying the HIPAA Security Officer of all incidents and/or potential breaches of PHI security. All reported incidents shall be appropriately documented. Security breaches shall be mitigated to the extent practicable and reported, as required under HIPAA and the amendments, rules and regulations, thereto.

- Town employees who access, receive, or otherwise handle or control PHI shall do so securely and responsibly pursuant to this Policy and the HIPAA Security Rule.

III. Enforcement

- Every Town employee with access to PHI shall 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.

552063/TOWN/0001

ADOPTED BY THE BOARD OF SELECTMEN ON January 24, 2017

Carolyn Smart, Chairman

Gordon Clark, Vice-Chair

Cindy King, Clerk