THE TOWN OF ESSEX
HIPAA SECURITY POLICY
FOR DESIGNATED HEALTH CARE COMPONENTS

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 Essex ("Town") hereby adopts this Security Policy for the departments, officials and employees designated as health care components ("Designated Health Care Components") in the Town's Designation of HIPAA Hybrid Entity Status, which Designation is expressly incorporated herein. This Policy sets forth the framework for the Designated Health Care Components' compliance with the Security Rule.

I. Purpose

The Security Rule defines the standards, which require covered entities, such as the Designated Health Care Components, 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 Designated Health Care Components' HIPAA security official is the Town Administrator.
- HIPAA Security Rule: The Security Rule establishes national standards for the security of 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 Designated Health Care Components 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 Designated Health Care Components. The HIPAA Security Official may, at his discretion, implement appropriate safeguards and procedures in furtherance of this Security Policy.

A. Administrative Safeguards

1. Security Awareness and Training
    - All Designated Health Care Components, including its officials and employees, who are authorized to view, send, receive or manage PHI shall undergo HIPAA training.
2. Workforce Security
    - Only authorized Designated Health Care Components' officials or employees shall have access to systems that manage, view, send or receive PHI.
    - Designated Health Care Components shall, at their discretion, limit authorized personnel's access to PHI to the extent that access to this information is necessary to fulfill the requirements of the person's job responsibilities.
    - Designated Health Care Components shall implement procedures for terminating an authorized individual's access to PHI when the individual's employment terminates or when the job responsibilities of the person no longer require that individual to access PHI.
    - Designated Health Care Components shall review systems in place to ensure that only currently authorized personnel have access to systems containing PHI.
3. Information Access Management
    - Only authorized personnel at Designated Health Care Components shall have access to systems that contain, manage, send and/or receive PHI in Town.
    - A department designated as a Designated Health Care Component and all officers and employees thereof are prohibited from releasing PHI to any other official, employee or department of the Town, unless there is a written HIPAA authorization or unless otherwise allowed by law.

4. Password Management

- Designated Health Care Components' officials or employees with access to PHI shall, at all times, maintain secure password management of their computers. In furtherance of this Policy, employees should choose a password that is difficult to guess and uses between six and eight characters.
- Passwords shall be regularly changed.
- Designated Health Care Components' officials and employees shall, at all times, keep their passwords secure and private. Employees shall not share or authorize another employee to login to their computer, documents or network using his/her password.
- In the event that a Designated Health Care Component's 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

- Designated Health Care Components shall ensure that systems that send, maintain, manage or receive PHI are kept in secure areas with physical security controls in place that 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 office or 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 Designated Health Care Components' 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 access PHI.

3. Record Retention/Disposal

- Under the Privacy Rule, Designated Health Care Components shall maintain, to the extent permitted by law, HIPAA policies and procedures, actions, activities and designations made in either written or electronic form for at least six years, and for such additional period as may required by state law.
- Medical records shall be maintained in accordance with state law.

- Designated Health Care Components shall apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other PHI for whatever period such information is maintained by Designated Health Care Components, including through disposal.
- Designated Health Care Components, 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 for Designated Health Care Components shall comply with all Town HIPAA policies.
2. Password Protection
    - When Designated Health Care Components' officials or employee with access to PHI are away from their computers for extended periods, the computer station shall be secured with a password protected return from sleep or screen saver feature.
    - No computer that contains access to PHI shall remain logged on outside of an employee's office hours or when the work station is temporarily 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 used by a Designated Health Care Component, 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.
- 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. AOL, Gmail, Yahoo, Hotmail) shall never be used to conduct Designated Health Care Component business, including the transmission of messages or attachments, which contain PHI.
- If a Designated Health Care Component official or employee believes that sensitive data has been compromised in any manner, the employee shall immediately notify the HIPAA Security Officer.

D. Designated Health Care Components Responsibilities

- Designated Health Care Components' officials and 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.
- Designated Health Care Components' officials and 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 of Designated Health Care Components shall be mitigated to the extent practicable and reported, as required under HIPAA and the amendments, rules and regulations, thereto.
- Designated Health Care Components' officials and 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 Designated Health Care Component official or 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-time, 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.

THE TOWN OF ESSEX
HIPAA SECURITY POLICY
FOR DESIGNATED HEALTH CARE COMPONENTS

EMPLOYEE ACKNOWLEDGMENT:

I have read and understand this policy. If questions arise in the future, I will consult my supervisor and/or the Town Administrator before taking action regarding the topics covered herein.

_____ _____

Printed Name Date

_____

Signature