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

Introduction

The Town of Essex ("Town") hereby adopts this Privacy Policy for the departments, officials and employees designated as health care components ("Designated Health Care Components") as set forth in the Town's Designation of HIPAA Hybrid Entity Status, which Designation is expressly incorporated herein. Accordingly, the Town's Designated Health Care Components must comply with the Health Insurance Portability and Accountability Act of 1996's ("HIPAA") requirements, including this Privacy Policy adopted pursuant thereto.

HIPAA, as amended, as well as its implementing regulations, restrict the Town's Designated Health Care Components' 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 have its Designated Health Care Components fully comply with HIPAA's requirements, including the Privacy Rule, Public Law 104-191. To that end, all Designated Health Care Components who have access to PHI must comply with this Privacy Policy.

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 address the Town's Designated Health Care Components' 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 Person;
- 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;

- Designated Health Care Components' 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;
- Requests for Restrictions on Uses and Disclosures of PHI; and
- Enforcement.

The Town's Designated Health Care Components' Responsibilities as Covered Entities

I. The Town's Designated Health Care Components' Privacy Official/Contact Person

The Town Administrator shall be the HIPAA Privacy Official for the Town. The Privacy Official, and his designees, 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 Designated Health Care Components' PHI use and disclosure procedures. The Privacy Official and his designees shall also serve as the contact persons for individuals who have questions, concerns, or complaints about the privacy of their PHI.

II. Training for Officials and Employees of Designated Health Care Components

It is the Town's policy to train all Designated Health Care Components' officials and employees who have access to PHI on HIPAA's privacy and security policies and procedures. The Privacy Official and his designees are charged with developing training schedules and programs so that all Designated Health Care Components' employees receive necessary and appropriate training to adhere to HIPAA's requirements.

III. Technical and Physical Safeguards of PHI

Pursuant to this Policy, the Town's Designated Health Care Components shall establish appropriate technical and physical safeguards to prevent Designated Health Care Components from intentionally or unintentionally using or disclosing PHI 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 Designated Health Care Components' offices, files and workspace where

PHI is stored.

Appropriate technical and physical safeguards shall be designed to ensure that only authorized Designated Health Care Components' 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 that its Designated Health Care Components comply with HIPAA's Security Rule. 45 CFR 160, 162, and 164.

IV. Privacy Notice

The Privacy Official and his designees are responsible for developing and maintaining a notice of the Designated Health Care Components' privacy practices ("Notice of Privacy Practices") that describes:

- the uses and disclosures of PHI that may be made by Designated Health Care Components;
- individual rights; and
- Designated Health Care Components' legal duties with respect to the PHI.

The Notice of Privacy Practices shall inform individuals that Designated Health Care Components will have access to PHI in connection with its covered medical and administrative functions. In addition, the Notice of Privacy Practices will provide a description of the Designated Health Care Components' complaint procedures and the name and telephone number of the Privacy Official and his designees.

To the extent practicable, the Notice of Privacy Practices shall be available to all persons receiving medical attention or otherwise providing Designated Health Care Components with PHI subject to the protections of HIPAA, and a written acknowledgement of such delivery shall be sought and received:

- 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 ambulances and on the Town's website and made available upon request to the Privacy Official and his designees.

V. Complaints

The Privacy Official and his designees shall be the Designated Health Care Components' contact persons for receiving complaints concerning use and disclosure of PHI. The Privacy Official and his designees shall be responsible for creating a process for receiving, investigating and addressing complaints lodged with regard to Designated Health Care Components' 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 Designated Health Care Components' officials and employees, shall include the potential for termination.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

Designated Health Care Components 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 a Designated Health Care Component's official or 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, said individual shall immediately contact the 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 Secretary.

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

No Designated Health Care Component official or 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, Designated Health Care Components 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 Designated Health Care Components agree prior thereto to comply with the same restrictions and conditions that apply to the Town concerning use or disclosure of PHI through a Business Associate Agreement;
- PHI shall not be used or disclosed for employment-related actions or in connection with any other employee benefit plan;
- Report immediately or as soon as practicable to the Privacy Official and his designees 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 Designated Health Care Components' 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 Designated Health Care Components' privacy policies and procedures shall be documented and maintained for at least six years and otherwise as required by 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, Designated Health Care Components 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 by Designated Health Care Components

I. Use and Disclosure Defined

Designated Health Care Components 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 a Designated Health Care Component, or by a Business Associate (defined below) of a Designated Health Care Component.
- *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 a Designated Health Care Component to have access to PHI.

II. Designated Health Care Components Must Comply With This Privacy Policy

All Designated Health Care Components 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 Designated Health Care Components in Town

- Designated Health Care Components with access to PHI shall not disclose PHI to any other individual, entity, Town Department, official or employee who has not been designated as a health care component in the Town's Designation of HIPAA

Hybrid Entity Status unless an authorization has been provided and/or the disclosure is otherwise is in compliance with this Policy and/or otherwise allowed by law.

- If an employee or official of a Town Designated Health Care Component performs duties for both the health care component as an employee or official of such component and for a non-health care component of the Town in the same capacity with respect to that component, such employee or official shall not use or disclose PHI created or received in the course of or incident to the employee or official's work for the health care component in violation of HIPAA.

IV. Permitted Uses and Disclosures

The Town's Designated Health Care Components, as "covered entities" for purposes of HIPAA, are 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 Designated Health Care Component'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 Designated Health Care Components' own health care operations. PHI may be disclosed between Designated Health Care Components or external covered entities 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 Designated Health Care Components' 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 by Designated Health Care Components 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, Designated Health Care Components shall not 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 authorized personal representative) authorizes in writing.

VI. Mandatory Disclosures of PHI

An individual's PHI shall be disclosed under HIPAA in two situations:

1. The disclosure is to the individual who is the subject of the information; and
2. 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

Designated Health Care Components 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 Designated Health Care Component shall review with a 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;

- Law enforcement purposes;
- Decedents;
- Cadaveric organ, eye or tissue donation;
- Research;
- Serious threat to health or safety;
- Essential government functions;
- Workers' Compensation.

VIII. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed by Designated Health Care Components for any purpose 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 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 an Designated Health Care Component official or employee requests disclosure of PHI from 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 a 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

Designated Health Care Components may disclose PHI to their business associates and allow Designated Health Care Components' business associates to create or receive PHI on its behalf. Prior to creating or receiving PHI, Designated Health Care Components 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," Designated Health Care Components shall contact the 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 Designated Health Care Component's function or activity involving the use and disclosure of PHI (including claims processing or administration, data analysis, underwriting, etc.); or
- provides medical, legal, accounting, actuarial, consulting, data aggregation, 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

Designated Health Care Components 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 Designated Health Care Components or their business associates maintain in designated record sets.

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 Designated Health Care Components accept 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, Designated Health Care Components must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. The Privacy Rule specifies processes for requesting and responding to a request for amendment. Designated Health Care Components 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 Designated Health Care Components' 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 Designated Health Care Components or their business associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request, except that Designated Health Care Components 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. Requests for Restrictions on Uses and Disclosures of PHI

- **Restriction Request.** Individuals have the right to request that a covered entity restrict use or disclosure of their 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. Designated Health Care Components are under no obligation to agree to requests for restrictions. If a Designated Health Care Component does agree, it must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.

- **Confidential Communications Requirements.** Designated Health Care Components shall permit individuals to request an alternative means or location for receiving communications of PHI by means other than those that Designated Health Care Components typically employ. For example, an individual may request that Designated Health Care Components 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.

IV. Enforcement

- All Designated Health Care Components with access to PHI, as set forth in the Town of Essex's Designation of HIPAA Hybrid Entity Status, are 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-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.

413331/ESSX/0001

THE TOWN OF ESSEX

HIPAA PRIVACY 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