

**CITY OF NORTH ROYALTON  
IDENTITY THEFT PREVENTION PROGRAM  
FOR  
EMERGENCY MEDICAL SERVICES**

The City of North Royalton (“City”) has approved and adopted this Identity Theft Prevention Program (“Program”). This Program has been developed in accordance with the Federal Trade Commission’s Identity Theft Prevention Red Flag Rules (16 CFR § 681.2). This Program has been created after conducting an assessment of the risks of Identity Theft associated with certain accounts that arise as a result of providing emergency medical services to individuals within the City.

**I. Definitions**

For purposes of the Program, the following terms are defined as:

- A. “Covered Account” means (i) any account the City offers or maintains primarily for personal family or household purposes that involves multiple payments or transactions or one or more deferred payments (which includes payment deferred while insurance claims are pending) and (ii) any other account the City identifies as having a reasonably foreseeable risk to customers. The City has identified Covered Accounts for purposes of this Program as being all accounts for which the City provides medical services and bills the Patient at a time subsequent to such services.
- B. “Emergency Medical Services (EMS) Personnel” means any employee of the City’s Fire Department and all City employees that work with, or are responsible for, EMS billing accounts.
- C. “Identity Theft” means fraud committed using the identifying information of another person.
- D. “Patient” means any person with whom EMS Personnel interact with for the purpose of providing that person with medical treatment.
- E. “Red Flags” mean a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

**II. Program Purposes**

The purposes of the Program are to:

- 1) Identify the relevant Red Flags based on the risk factors associated with the City’s Covered Accounts;
- 2) Institute policies and procedures for detecting Red Flags;
- 3) Identify steps the City, its administration, and/or outside service providers will take to prevent and mitigate Identity Theft; and
- 4) Create a system for regular updates and administrative oversight of the Program.

**III. Identification of Red Flags**

Red Flags generally fall within one of the following four general categories:

- 1) Suspicious documents;
- 2) Suspicious personal identifying information;
- 3) Suspicious or unusual use of a Covered Account; and
- 4) Alerts from others (e.g. customer, Identity Theft victim, or law enforcement).

“Column A” of the attached Appendix A is a list of some Red Flags that would be most relevant to the City for purposes of the services provided by the EMS Personnel.

#### IV. Detection of Red Flags

In order to facilitate detection of Red Flags, EMS Personnel will take steps to obtain and verify the identity of the Patient. However, this Program recognizes that the circumstances of each situation requiring emergency medical services will vary and will require differing degrees of urgency. **Although EMS Personnel are required to take the steps when circumstances allow, no step should be taken if that step would detrimentally interfere with, or delay, the provision of medical services to the Patient or would cause unreasonable discomfort or stress to the Patient.**

When treating a Patient, EMS Personnel must:

1. Ask the Patient for his/her name, home address, date of birth, and social security number. If the Patient is unable to provide this information, ask nearby persons. Record the information.
2. If there is minimal urgency, ask the Patient for a photo ID. If the Patient presents a photo ID, verify the name, address, and date of birth against the information provided verbally by the Patient. If different than the information given by the Patient, record the differences. If the Patient presents a driver's license, record the license number and state of issuance.

**NOTE:** Refusal or failure to provide a photo ID will not affect the provision of medical services.

All information must be cross-referenced with any insurance information and the Patient Registration Face Sheet created at the treating medical facility. Discrepancies in personal identifying information should be reviewed for Red Flags.

#### V. Preventing and Mitigating Identity Theft

- A. When a Red Flag arises, supervisory EMS Personnel will take appropriate steps to investigate the Red Flag to determine if there is credible evidence of identity theft. Such steps are set forth in "Column B" of the attached Appendix A.
- B. If credible evidence of identity theft is found, EMS Personnel shall notify the Fire Chief immediately of the situation. The Fire Chief shall instruct on the appropriate steps to prevent the continuation of the Identity Theft and to mitigate damages arising from the Identity Theft. Such steps may include:
  - 1) Informing the individual whose identity has been used and assisting that individual in taking actions to mitigate damage from the identity theft, such as by providing information to third parties, if requested to do so by the individual.
  - 2) Stop billing and collections on the account with respect to the Identity Theft victim.
  - 3) Notify law enforcement.
  - 4) Any other action deemed appropriate by the Fire Chief or Mayor.
- C. Future Outside Service Providers
  1. On the effective date of this Program, the City does not use an outside service provider ("Service Provider") for Patient billing.
  2. If the City decides to use a Service Provider after the adoption of this Program, the City will require each Service Provider to implement its own identity theft prevention policy in accordance with the FTC's Red Flags Rules. The City will review the Service Provider's policy and will require changes to said policy, as it pertains to the City's billing accounts, when needed. ("Column B" of the attached Appendix A details examples of the types of mitigation and resolution procedures that should be contained in the Service Provider's policy.)
  3. The Service Provider's policy shall include the following provisions:

- a.) That all Red Flags be responded to in accordance with the Service Provider's identity theft prevention policy.
  - b.) That all Red Flags which are not reconciled upon initial review of Service Provider staff be escalated to supervisory staff for further investigation.
  - c.) That when there is verification of a Red Flag by the supervisory staff, and it appears that there is credible evidence that identity theft has occurred, the Service Provider shall inform the City of such in writing and take action on the account only in accordance with the City's direction.
4. The Fire Chief will designate a supervisory level employee to be responsible for coordinating with the Service Provider and other City employees and officials on possible Identity Theft situations.

**VI. Program Administration and Training**

The Fire Chief, with the assistance of the City Director of Law, is responsible for developing, implementing, administering and updating the Program. The Fire Chief, or his/her designee, will be responsible for developing a training program for EMS Personnel and other City employees identified by the Fire Chief as having a role in implementing the Program. Training on this Program shall occur upon hiring of EMS Personnel and on an "as needed" basis thereafter. A record of training shall be kept by the Fire Chief.

**VII. Updating of Program**

The Fire Chief will periodically review the effectiveness of the Program and update the Program to reflect the addition or removal of Covered Accounts, and changes in risks to Patients from Identity Theft. An annual report shall be provided by the Fire Chief to the Mayor regarding significant incidents involving Red Flags and the City's response, the effectiveness of the Program, and recommendations for change.

Signed into effect by:

\_\_\_\_\_  
Mayor Robert A. Stefanik

Date: \_\_\_\_\_

Adopted by City Council through Resolution No. \_\_\_\_

Passed \_\_\_\_\_

Acknowledged by:

\_\_\_\_\_  
Fire Chief

Date: \_\_\_\_\_

Appendix A

EXAMPLES OF IDENTITY THEFT RED FLAGS (Column A)	EXAMPLES OF PREVENTION/MITIGATION PROCEDURES (Column B)
Documents provided for identification appear to have been altered or forged.	Stop the billing process and require Patient to provide additional satisfactory information to verify identity.
Personal identifying information provided by the patient is not consistent with other personal identifying information provided. For example, there is a lack of correlation between the Social Security Number (SSN) range and date of birth.	Stop the billing process and require Patient to provide additional satisfactory information to verify identity.
The SSN provided is the same as that submitted by a different person in the past.	Stop the billing process and require Patient to provide additional satisfactory information to verify identity.
Patient has an insurance number but never produces an insurance card or other physical documentation of insurance.	Require Patient to provide additional satisfactory information to verify identity.
Complaint/inquiry from an individual based on receipt of: -a bill for medical services for another individual; -a bill from a medical provider that the Patient never used; - a notice of insurance benefits (or Explanation of Benefits) for health services never received.	Stop billing process and investigate complaint.
Complaint/inquiry from a Patient about information added to a credit report by EMS or insurer and Patient denies receiving the services.	Investigate complaint.
Complaint/inquiry from a Patient about the receipt of a collection notice related to the account and Patient denies receiving services.	Investigate complaint.
Patient or insurance company report that coverage for legitimate services is denied because insurance benefits have been depleted or a lifetime cap has been reached and the Patient states that he/she has not utilized insurance to that extent.	Investigate complaint.
Mail sent to the Patient is returned repeatedly as undeliverable although Patient continues to use the address in connection with the Patient's account.	Investigate discrepancy.
Health care provider is notified of a possible fraud or identity theft by an individual whose identity has been used, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.	Stop billing on account and attempt to identify proper party on the account; cooperate with the victim.