



# E. John Gavras Center

Cerebral Palsy Associations of Cayuga County Inc.

Richard M. Hansinger  
Executive Director

www.gavrascenter.com

888-255-2746 or 315-255-2746  
Fax: 315-255-2740

182 North Street  
Auburn, NY 13021

## IDENTITY THEFT PREVENTION PROGRAM POLICY AND PROCEDURE

### I. Purpose.

This policy and procedure statement is designed to detect the warning signs, the “red flags,” of identity theft in the day to day operations of the Agency, to take steps to prevent identity theft, and to mitigate the damage if it is detected. In this document, the Agency describes the recommended measures to be followed when services are sought to be obtained, or are obtained, under a fictitious name or in another person’s name.

### II. Policy.

The Agency strives to prevent the intentional or inadvertent misuse of person’s name, identities, identifying information and medical records; to report criminal activity relating to identity theft and theft of services to appropriate authorities; and to take steps to correct and/or prevent further harm to any person whose name or other identifying information is used unlawfully or inappropriately.

### III. Definition.

**Identity theft** means the act of: knowingly obtaining, possessing, buying, or using, the personal identifying information of another: (i) with the intent to commit any unlawful act including, but not limited to, obtaining or attempting to obtain credit, goods, services or medical information in the name of such other person; and (ii)(a) without the consent of such other person; or (b) without the lawful authority to obtain, possess, buy or use such identifying information.

### IV. Signs of Possible Identity Theft (Identification of Red Flags).

The Agency staff should be alert for cases of possible identity theft. Identify theft can arise in a myriad of different ways; some of the most common are:

**1. Suspicious Documents.** Paperwork presented by the person can have signs of identity theft. Examples of red flags involving documents include:

A. Identification documents that look altered or forged.

B. The person presenting the identification doesn’t look like the photo or match the physical description on the documents; for example, the person’s Medicaid card or other photo or description does not match the person.

C. Information on the identification document differs from what the person presenting the identification is telling you and doesn’t match other information presented or on file with the Agency. For example, the name, address, phone number, social security number or other identifying information does not match what the person is telling you, or is identical to information provided by another person.

D. A person presents an application or other document that appears to have been altered, forged or torn up and reassembled.

**2. Suspicious Personal Identifying Information.** Identity thieves may use personally identifying information that appears to be false. Among the red flags involving identifying information are:

A. Inconsistencies with other information already on file regarding the person. An example would be a person appearing and giving an identity that has been flagged in the Agency's records as suspect, or has been documented previously or communicated previously to the Agency by another person or entity to be related or connected to known fraudulent activity (known false names / addresses / telephone number / social security numbers, etc.); or the same information provided by multiple persons.

B. Inconsistencies in the information the person has given you. For example, the name, social security number, Medicaid information, etc. differs from the information previously provided by the person.

C. A person who omits personally identifying information from a form he or she is asked to complete, and / or does not respond to notices that the forms are incomplete.

D. A person who cannot provide authenticating information beyond what is generally available in a wallet; for example, the person cannot answer a challenge question.

**3. Suspicious Activity.** Red Flags may arise in the course of the use of the personally identifying information. Some of the more common examples are:

A. A long-dormant account is suddenly reactivated with no reasonable explanation.

B. Mail sent to the person is returned repeatedly as undeliverable although the account continues to be used.

C. The Agency receives information that unauthorized users are using the account, that there are unauthorized charges that statements are not being received by the person, or the Agency is notified by the person or his / her representatives that identity theft has occurred.

D. Family members / friends call the person by a name different than that provided by the person at registration.

## **V. Procedures to detect red flags.**

### **A. New Persons.**

The Agency must make reasonable efforts to verify the identity of new people, including but not limited to confirming the name, address, telephone number, private insurance number, social security / Medicaid identification number, etc. Depending on the circumstances, the Agency can confirm the consumer's identity by examining the person's drivers' license, passport, or other identifying documents. Information can be accessed from other sources, such as the Medicaid card, Social Security Death Index, (<http://ssdi.rootsweb.ancestry.com/>) reports from law enforcement or credit agencies, etc., if necessary.

### **B. Existing Persons.**

Each time the person presents him / herself for service, the Agency will make reasonable efforts to authenticate the identity of the person, and will monitor the person's account by being alert to changes of address, insurance coverage, etc.

## **VI. Prevention and Mitigation of Identity Theft.**

If the Agency detects identity theft, it will make reasonable efforts to respond. Some of the responses may include the following:

1. 'Flagging' the account and monitoring the account for future use.
2. Contacting the person and / or his / her representative. The Agency may notify the person using the "FTC Letter", and assist the person in completing the "FTC Identity Theft Affidavit".
3. Changing passwords, security codes, or other ways that the person's account may be accessed.
4. Closing the account.
5. Reopening the account with the correct information.
6. Notifying law enforcement, and / or the Medicaid Inspector General or other regulatory agencies.
7. Not opening the account.
8. Correcting inaccurate information contained in a person's record, and notifying other area health care providers, only after receipt of the completed FTC Identity Theft Affidavit.
9. If known to the Agency, the Agency may bill the identity theft suspect for unlawfully obtained services. If the Agency has suffered an ascertainable loss, the Agency may consider appropriate legal action.
10. Under the appropriate circumstances, the Agency may choose to do nothing at the time the particular identity theft is detected.

## **VII. Procedures.**

### **A. When Identity Theft is Alleged,**

1. Flag the account as suspected identity theft-related, so that Administrative staff and Program Coordinators know that the medical record may contain inaccurate information. Notify the Agency Compliance Officer of the suspected theft.
2. Advise and assist the victim to report identify theft to law enforcement. The Agency by way of the Executive Director may independently report identity theft to law enforcement and or regulatory authorities, including the Medicaid Inspector General, if appropriate.
3. Complete and send the victim the FTC Identity Theft Letter and assist the victim or legal guardian in completing the FTC Identity Theft Affidavit.
4. Follow the remainder of the steps below when identity theft is reasonably suspected, or known to have occurred.

## **B. When Identity Theft is Reasonably Suspected or Known to have Occurred.**

1. Complete the Identity Theft Reporting Form; provide copies to the Agency Compliance Officer or other appropriate staff.
2. Place the person's account on hold pending the outcome of an investigation or resolution.
3. The Compliance Officer or other authorized individual will determine the nature and extent of investigation and reporting based upon the facts and circumstances of the matter.
4. The Agency may notify an unknowing victim of identity theft and provide them with a copy of the FTC Identity Theft Affidavit.
5. Correct the medical record and billing records as appropriate after receipt of the completed FTC Identity Theft Affidavit.

## **VIII. Program Administration.**

1. This Policy and Procedure Statement shall be approved by the governing body of the Agency.
2. The Agency shall provide training on this Identity Theft Prevention Program to appropriate staff, volunteers, vendors and business associates.
3. The Agency shall monitor the implementation and operation of the Identity Theft Prevention program. The Agency shall make annual reports on the identity Theft Prevention program to the Board of Directors
4. The Agency shall appoint a particular individual or individuals to monitor, oversee and evaluate the Identity Theft Prevention Program.
5. The Agency shall develop standards and protocols for investigation of suspected identity theft and reporting of identity theft to law enforcement officials.

## **IX. Resources**

US Federal Trade Commission, Fighting Fraud With the Red Flags Rule - A How-To Guide For Business. <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>

### **Federal Trade Commission Identity Theft Affidavit**

Copies may be obtained from: <http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf>