



Identity Theft Prevention and Detection Program

Applicability: This program applies to all Oak Hill employees, managers, supervisors and directors.

Purpose: Oak Hill is responsible for protecting our program participants from identity theft. The purpose of this Identity Theft Prevention Program (the "Program") is to detect, prevent, and mitigate identity theft in connection with new and existing medical and financial accounts of our program participants. This Program is required pursuant to the Federal Trade Commission's "Red Flag Rules", as set forth in Title 16 of the Code of Federal Regulations, §681.1. Oak Hill will implement this Program in order to combat identity theft in connection with the medical and financial accounts of existing and new program participants.

The Program

A. Program Development, Implementation and Reporting

1. Oak Hill's Board of Directors will approve the initial Program.
2. Oak Hill's Senior Management Cabinet will be involved in the oversight, development, implementation and administration of the Program.
3. The Compliance Officer is the designated individual who is responsible for the Program's oversight, development, implementation and administration.
4. The Compliance Officer will provide annual reports to Oak Hill's Board of Directors and Senior Management Cabinet regarding Oak Hill's compliance with the "Red Flag Rules". The annual report will address material matters related to the Program and evaluate issues such as:
 - The effectiveness of Oak Hill's policies and procedures in addressing the risk of identity theft in connection with new and existing program participant accounts;
 - Performance of, and any issues related to, service provider arrangements;
 - Significant incidents involving identity theft and Oak Hill's response to such incidents; and
 - Recommendations for material changes to the Program.
5. The Compliance Officer will approve material changes to the Program as necessary to address changing identity theft risks.

6. Oak Hill will educate all employees on how to implement the Program.
7. Oak Hill will ensure that all service providers that perform activities in connection with one or more program participant accounts (i.e. collection agencies) are informed of their obligation to implement policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

B. Deterring Identity Theft.

Staff must take reasonable efforts to protect our program participants from identity theft. Refer to Oak Hill's policies regarding Confidentiality, Protecting Social Security Numbers and Document Retention for guidance. Examples of reasonable efforts include:

- Shred unnecessary financial and medical documentation with personal information.
- Do not leave computer screens unattended that display program participants' confidential information.
- Protect confidential information such as social security numbers by keeping the information in locked file cabinets, using encryption software provided by IT, and limiting the personal information that is shared via email and all other unsecured communication methods.
- Do not leave laptops unattended or visible in automobiles.

C. Identifying attempted identity theft or fraud.

In order to limit the risk that the identity of a program participant may be compromised, all Oak Hill staff should report any of these occurrences to the Compliance Officer or any other suspicious activity in connection with the delivery of services:

1. The social security number furnished by the program participant has not been issued, is listed on the Social Security Administration's Death Master File, or is otherwise invalid. Additional information may be found on the Social Security Administration's website. The following numbers are always invalid:
 - The first three digits are in the 800, 900, or 000 range, 700 range above 772, or are 666;
 - The fourth and fifth digits are 00; or
 - The last four digits are 0000.
2. Personal identifying information given by the program participant is not consistent with personal identifying information in Oak Hill's records.
3. The social security number or other identifying information furnished by the program participant is the same as identifying information in Oak Hill's records furnished by other individuals.

4. Mail sent to the program participant is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the program participant's account.
5. A program participant has an insurance number but never produces an insurance card or other physical documentation of insurance.

D. Detecting Identity Theft Red Flags

Oak Hill will, to the extent feasible, request documentation of the program participant's identity, residence address, and insurance coverage at time of registration. Staff should be suspicious of mail, email or other documents relating to program participants' financial accounts that are out of the ordinary and which may be evidence that their identity has been compromised. Examples include: unexpected credit cards or account statements; call or letters regarding purchases that were not made.

E. Investigating Suspected Identity Theft

Oak Hill will investigate situations in which it determines that one of its program participants is likely to be the perpetrator or the victim of identity theft. If, following the investigation, Oak Hill determines that one of its program participants has been a victim of identity theft, Oak Hill will notify the program participant's family or guardian (if the program participant is unaware of the identity theft). If there is evidence to believe that identity theft has occurred, Oak Hill will file a police report for identity theft on behalf of the program participant.

1. The parent/guardian will be asked to complete one of the following documents:
 - the ID Theft Affidavit developed by the Federal Trade Commission, including supporting documentation; or
 - an ID theft affidavit recognized under state law; or
 - a statement including the following information:
 - A statement that the program participant is a victim of identity theft;
 - Any other identification document that supports the statement of identity theft;
 - Specific facts supporting the claim of identity theft, if available;
 - Any other explanation that the program participant did not incur the debt;
 - Any available correspondence disputing the debt;
 - Documentation of the residence of the program participant at the date of service,
 - A telephone number for contacting the program participant;
 - Any information that the program participant may have concerning the person who registered in his or her name, his or her name or personal information for obtaining services; or
 - A statement certifying that the representations are true, correct, and contain no material omissions of fact to the best knowledge and belief of the person submitting the certification.

2. The parent, guardian, and/or program participant must cooperate with comparing his or her personal information with information in Oak Hill's records.
3. Oak Hill will take the following steps:
 - If the program participant's account had been referred to a collection agency or attorney for collection, the collection agency/attorney will be instructed to cease collection activity.
 - Close any account that has been opened fraudulently and open a new account for the program participant.
 - cooperate with any law enforcement investigation relating to the identity theft.
 - notify any insurance company, government program or other payor that has made payment on the account.
 - notify a consumer reporting agency that the account was not the responsibility of the program participant (if an adverse report had been made to a consumer reporting agency).
 - Place a "fraud alert" on the program participant's credit reports
 - Oak Hill will change any passwords, security codes, or other security devices that permit access to the account.
 - Oak Hill will monitor the account for future identity theft.
4. If following investigation, it appears that the program participant has not been a victim of identity theft, Oak Hill or the collection agency will give written notice to the program participant that he or she has not been the subject of identity theft. The notice will state the basis for determining that the person claiming to be a victim of identity theft was in fact the program participant who received services from Oak Hill.
5. In the event there is an unauthorized access of electronic data that contains personal information (social security number or account number in combination with a password or security code that would permit access to such account) that has not been secured by encryption or another method that renders such information unreadable or unusable, Oak Hill will notify the parent or guardian of the program participant (whose information was accessed) of such unauthorized access if it is determined that the unauthorized access will likely result in harm to the program participant. Such notification will be made without unreasonable delay.

F. Disposition of Medical Record When Identity Theft Is Confirmed

Oak Hill will correct errors in medical records that are the result of identity theft. If it is confirmed that a program participant's record was created as the result of identity theft, a notation concerning the identity theft will be placed in the record. All demographic information will be removed from the record. Staff will determine whether any other records are linked to the record found to be created through identity theft.

In some cases, identity theft may involve an identity thief receiving care under the name of another person, who has been a program participant. In such a case, other files relating to the

program participant will be reviewed and any information relating to the identity theft will be removed and segregated.

G. Updating the Identity Theft Prevention Program

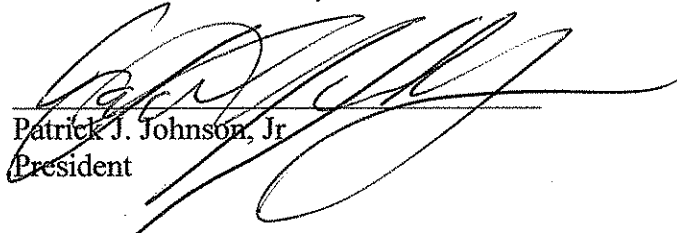
The Program will be updated to reflect the most recent changes in risk of identity theft to program participants and Oak Hill. The Compliance Officer will evaluate these policies on an annual basis and update such policies as necessary to reflect changes in risks of identity theft to program participants or Oak Hill.

The Compliance Officer will consider the following factors when evaluating the policies:

- Changes in methods of identity theft and Oak Hill's experiences with identity theft;
- Changes in methods to detect, prevent and mitigate identity theft;
- Changes in the types of accounts that Oak Hill offers or maintains; and
- Changes in the business arrangements of Oak Hill (i.e. service provider arrangements, etc.).

This Program was approved on July 2, 2009

This Program is effective July 31, 2009



Patrick J. Johnson, Jr
President