



This document is intended to be a template which should be customized to fit the unique needs of the provider's operations.

Policy Template – Policy on Administration and Oversight of Red Flag Identity Theft Prevention Program

It is the policy of *[INSERT NAME OF PROVIDER/ORGANIZATION]* to have in place a Red Flag Identity Theft Prevention and Compliance Program. The program will be operable in facilities with oversight, reporting and updating of the program by senior management or officers.

I. Identification of Red Flags

- a. Red Flags are defined as: A pattern, practice, or specific activity that indicates the possible existence of identity theft. [15 USC 1681m(c)(2)(A)]
- b. The following risk factors are considered in identifying relevant Red Flags for covered accounts, as appropriate:
 - i. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
 - ii. The presentation of suspicious documents;
 - iii. The presentation of suspicious personal identifying information, such as a suspicious address change;
 - iv. The unusual use of, or other suspicious activity related to, a covered account; and
 - v. Notice from patients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
- c. Red Flags will be periodically examined for applicability.
- d. Red Flags may be added given industry trends and company experience and history with identity protection for covered accounts.
- e. Should a Red Flag be detected the incident will be addressed through authentication and verification of identifying information or requests and monitoring of transactions.

II. Covered Accounts

- a. Covered Accounts are defined as:
 - i. An account primarily for personal, family, or house hold purposes, that involves or is designed to permit multiple payments or transactions,
 - ii. Any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
- b. Covered Accounts will be monitored at initial opening and ongoing for the presence of an event or incident that may constitute a Red Flag.

III. Service Providers

- a. Service Provider is defined as:
 - i. A person that performs an activity in connection with a covered account on behalf of the facility. (Examples: collection agencies, billing companies).
- b. Service providers will be contractually obligated to take reasonable steps to detect, prevent, and mitigate the risk of identity theft of covered accounts. Any identified Red Flags will be reported to the facility for further appropriate action.



This document is intended to be a template which should be customized to fit the unique needs of the provider's operations.

IV. Mitigation/Response to Detected Red Flags

- a. If a Red Flag is detected and verified the facility will:
 - i. Report the Red Flag to the Compliance Department or the Privacy Officer. *[Insert proper approval level]*
 - ii. The responsible Department/Officer will determine an appropriate response which is commensurate with the degree of risk posed by the Red Flag and other aggravating factors such as data security incident, or other unauthorized access or release of information.

V. Program Approval and Oversight

- a. Upon development of the Red Flag Identity Theft Prevention and Compliance Program, the program will be submitted to senior management or officers for approval.
- b. Industry and company specific trends will be monitored for the need to modify the program or identified red flags.

VI. Program Reporting

- a. Periodically but not less than annually, a report will be made to the Board of Directors and to the Compliance Committee with regard to compliance, effectiveness, incidents and recommendations for revisions.
- b. Incidents discovered as result of Red Flag investigation findings will be escalated to the appropriate level and authority in accordance with Company policy as well as Local, State and Federal law.

VII. Periodic Updating of the Program

- a. The program will be reviewed annually and updated as required based on:
 - i. Changes to identity risks
 - ii. Company experience and history
 - iii. Content gathered to open a covered account
 - iv. Method by which information is gathered, stored or accessed
 - v. Change in the type of covered accounts

VIII. Program Training

- a. At inception of this program as well as for all program updates thereafter all individuals involved with gathering or accessing information will be trained according to their specific responsibility to protect identifying information.
- b. Program training will be a part of orientation and annual job specific training for applicable individuals.