



HEALTH CARE PROVIDER RED FLAGS RULE POLICY AND PROGRAM

PURPOSE

The Federal Trade Commission (FTC) has issued regulations, The Red Flags Rules, requiring financial institutions and creditors (includes most Health Care Providers, hereinafter referred to as the “**Institution**” or “**Provider**”), to develop and implement a written institutional Policy and Program (“**Program**”) as part of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

The Program must provide for the identification, detection, and response to patterns, practices, or specific activities, known as “red flags”, that could indicate identity theft regarding the opening of a covered account or any existing covered account. The Program will also coincide with this institution’s Health Insurance Portability and Accountability Act (HIPAA) Policy and Program.

The Provider’s Program must address four elements:

1. Identify relevant Red Flags as may be associated with Provider’s covered accounts;
2. Implement policies and procedures for detecting Red Flags;
3. Provider’s response to any detected Red Flags; and
4. Update the Program periodically to reflect changes in risk from identity theft to patients and to assess the Provider’s structure to prevent and mitigate identity theft.

The Program must also encompass the following mandates:

1. The Board of Directors, or an appropriate committee thereof, must approve the Institution’s initial Program;
2. Involvement of the Board of Directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the Program;
3. Train relevant staff as necessary, to effectively implement the program; and
4. Appropriate and effective oversight must be exercised by the Institution regarding service provider arrangements.

In addition to providing methods to *verify* an individual’s personal identifying information, the Program must also provide elements designed to *authenticate* the actual identity of the individual presenting said information by employing external public resources and data.

SCOPE

Medical identity theft, particularly involving insider access to data, is expressly addressed in the Red Flags Guidelines and directs Providers to monitor all circumstances to prevent and mitigate patient identity theft. Although many of the Red Flags Rule provisions apply to banks, credit unions, transportation dealerships, and other institutions, health care providers (whether for-profit, non-profit, or governmental entities) may have obligations under the Red Flags Rule based on the Rule’s definition of “Creditor”:

- any entity which regularly extends (offers), renews, or continues credit;
- any entity which regularly arranges for the extension, renewal, or continuation of credit; or
- any assignee of an original creditor which participates in the decision to extend, renew, or continue credit.

Essentially, if a health care provider offers credit to a consumer by establishing an account that permits multiple payments, the Provider is a “*creditor*” offering a “*covered account*”, and is subject to the Red Flags Rule.

For those health care providers employing consumer credit reports, the user must be prepared to take appropriate action when a “Notice of Address Discrepancy” is displayed on the report. The Provider must perform procedures designed to form a reasonable belief that a credit report relates to the consumer about whom the report was requested, and the Provider must then report the correct address to the Credit Reporting Agency.

DEFINITIONS

- a. **Financial Institution** - A state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a “transaction account” belonging to consumer.
- b. **Transaction Account** - Is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.
- c. **Creditor** - Defined as:
- i. is any entity that regularly extends (offers), renews, or continues credit;
 - ii. any entity that regularly arranges for the extension, renewal, or continuation of credit; and
 - iii. any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.
- Creditors include, but are not limited to: health care providers, finance companies, transportation dealers, mortgage brokers, utility companies, telecommunication companies, and most departments stores.
- d. **Account** - Is established as a person engaging a financial institution to obtain a product or service for personal, household or business purposes.
- e. **Covered Account** - Is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. Covered accounts include:
- i. emergency/non-emergency patient billing
 - ii. patient payment plans
 - iii. patient medical/insurance information
 - iv. credit card accounts
 - v. mortgage/transportation loans
 - vi. margin accounts
 - vii. cell phone accounts
 - viii. utility accounts
 - ix. checking/savings accounts
 - x. deferred payment situations
- A “covered account” is also an account for which there is a foreseeable risk of identity theft - for example, small business or sole proprietorship accounts.
- f. **Identity Theft** - Potential identity theft acts are defined as:
- i. *Identity fraud* - Identity fraud is the act of a person creating a fictitious identity or manipulating an existing identity to evade detection.
 - ii. *Identity theft* - Occurs when a person wholly takes over another individual’s identifying information.
 - iii. *Account takeover* - Is the act of a person obtaining an individual’s personal information (usually at a minimum, social security number {SSN}, account numbers, etc.) for the purpose of changing another person’s address with a financial institution. This illegal act creates a window of opportunity to perform financial transactions sent to a fictitious address before detection.
- g. **Medical Identity Theft** - Occurs when someone use’s a person’s name and sometimes other parts of their identity (*insurance information, SSN, etc.*) without the victim’s knowledge or consent to obtain medical services or goods, or when someone uses the person’s identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.
- h. **Identifying Information** - Defined as any identifying information which may be used to identify a person, such as:
- i. name
 - ii. social security number
 - iii. state issued driver’s license or ID
 - iv. employer or tax identification number
 - v. passport information
 - vi. unique biometric data
 - vii. unique electronic ID number, address, routing code
 - viii. telecommunication ID information or access code
- i. **Red Flag** - A pattern, practice or specific activity that indicates the existence of identity theft.

ANALYSIS OF RED FLAGS RISKS

The Institution will initially, and at least annually, examine and analyze the following relevant procedures and data regarding any indication of valid Red Flags as set forth herein:

- the Institution's previous experiences with identity theft or any relevant identity theft practices currently in use.
- the types of covered accounts offered or maintained by the Institution.
- the methods or practices provided to open and maintain covered accounts.
- the methods or practices provided to access covered accounts.
- individual's application for covered account.
- individual's credit report.
- any and all relevant documentation and sources for indications of identity theft Red Flags.

PROGRAM ELEMENT ONE

Identifying Red Flags

a. LEVEL 1 - INITIAL IDENTITY VERIFICATION.

i. Institution staff will initially confirm each covered account's identity by close inspection of the individual's presented driver's license or other ID employing the PLEASE method:

P = PICTURE. *Compare carefully to the individual presenting ID.*

L = LOGOS. *Also holograms. Are they present and unaltered.*

E = EXPIRATION DATE. *An out-of-date ID is invalid under any circumstances.*

A = AGE. *Compare displayed date of birth to the age of individual presenting ID.*

S = SIGNATURE. *Compare to any signature in-house, especially application for a covered account.*

E = EVIDENCE OF TAMPERING. *Review carefully for any suspicious alterations.*

ii. In states where applicable, a copy of the individual's ID will be retained for a period of five (5) years after the account is closed.

c. LEVEL 2 - ALERTS, NOTIFICATIONS OR WARNINGS FROM A CONSUMER REPORTING AGENCY.

i. Any fraud alert that is included within a consumer report at which time Institution staff must perform required actions as indicated by the alert.

ii. A CRA reports a Notice Of Credit Freeze.

iii. A CRA reports a Notice Of Address Discrepancy or if individual's address from presented ID does not coincide with any known address displayed on CRA report.

iv. The consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of the individual's activity, such as:

- a recent and significant increase in the number of report inquiries.
- an unusual number of recently established credit relationships.
- a material change in the use of credit, especially with respect to recently established credit relationships.
- an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

d. LEVEL 3 - SUSPICIOUS DOCUMENTS.

i. Suspicious documents may include, but are not limited to:

- Documents presented for identification appear to have been altered or forged.
- The photograph or physical description on the ID is not consistent with the appearance of the individual.
- Other information is not consistent with the information provided by the individual.
- Other information on the ID is not consistent with information previously on file at the Institution, including signature cards, recent check or previous documentation.
- An insurance information card appears to have been altered or forged.