

1. BACKGROUND AND SUMMARY

The Oregon Health & Science University (OHSU) Identity Theft Prevention Program is developed pursuant to the Federal Trade Commission's (FTC) "Red Flags Rule". The rule requires financial institutions and creditors such as OHSU holding certain types of accounts to develop and implement an identity theft prevention program.

2. PURPOSE

To establish a program to identify, detect and respond to "Red Flags" developed to recognize the patterns, practices or specific activities that indicate the possible existence of identity theft in connection with a covered account.

3. POLICY

All OHSU departments or units involved in the process or management of covered accounts must implement procedures to be consistent with the OHSU Red Flag Program as outlined below.

4. DEFINITIONS

- A. *Identity Theft*: a fraud committed or attempted using the identifying information of another person without authority.
- B. *Red Flag*: a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
- C. *Covered Account*: a patient, student or other type of account receivable designed to permit multiple payments or transactions to OHSU such as student accounts or a loan that is billed or payable monthly and administered by the University or a patient account where patients are allowed to defer payments or make installments over time, including billing for prior services rendered. Covered accounts do not include institutional accounts or accounts where the customer is not responsible for payment.
- D. *Program Administrator*: the individual or office designated with primary responsibility for oversight of the program.

- E. *Identifying Information:* any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or student identification number.

5. RED FLAG IDENTITY THEFT PREVENTION PROGRAM

OHSU's Red Flag Program contains the following four elements: (1) identify relevant Red Flags applicable to new or existing covered accounts; (2) detect the Red Flags as they occur in covered accounts; (3) initiate appropriate response to detected Red Flags to prevent and mitigate identity theft; and (4) periodically update the program.

6. IDENTIFIED RED FLAGS

Red Flags are potential indicators of fraud. Red Flags in each of the listed categories are listed on the OHSU Integrity web site. The examples are illustrative but not exclusive of Red Flags that may be considered for protocols specific to the OHSU department or unit.

- A. Notifications and warnings from credit reporting agencies;
- B. Suspicious documents;
- C. Suspicious Personal Identifying Information;
- D. Suspicious Covered Account activity or unusual use of account;
- E. Alerts from others.

7. DETECTING RED FLAGS

Each Department that is responsible for processes related to a covered account will document and implement a protocol to detect Red Flags. In order to detect relevant Red Flags, each Department should consider the types of accounts it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft.

The following OHSU functions should include but not be limited to:

- A. Registration processes to establish or update accounts.
- B. Management of existing accounts.
- C. Management of new accounts

8. RESPONSE AND MITIGATION

For all suspected or confirmed Red Flag incidents, the Department will follow the following protocols and procedures regarding Red Flags:

- A. The reporting procedures present in the Information Security Directive ISD-700-00017, *Information Security Incident Reporting Procedures*.
- B. With a detected Red Flag or a situation closely resembling a Red Flag investigation by the Department for verification; if a Red Flag or similar suspicious activity is confirmed, follow ISD-700-00017.
- C. Incidents identified as more than procedural or documentation errors should be reported to the Integrity Office. Contact information for reporting options available to individuals and may be included in unit or department Red Flag Program protocols:
 - Supervisor or Manager
 - Compliance Hotline 1-877-733-8313
 - Integrity Office 4-8849
 - Office of Public Safety 4-4444
 - ITG Help Desk 4-2222
- D. To assist with confirming the identification of customers, refer to Appendix A – *Identity Verification for “Red Flag” Covered Accounts*

9. PROGRAM ADMINISTRATOR

A. OVERSIGHT

The OHSU Integrity Office is responsible for developing, implementing, maintaining and periodically updating the Red Flag Program. The Integrity Office will provide such annual or periodic reports as required by regulation.

B. STAFF TRAINING AND REPORTS

Each Department responsible for a Covered Account is responsible to train staff concerning Red Flag Protocols. The Integrity Office will facilitate education about the Red Flag Program and updates.

Background:

Related policies, procedures and forms:

- **Appendix A: Identity Verification for “Red Flag” Covered Accounts**
- **Information Security Directive 700-00017**

Responsible office: Integrity Office
