Office of Employee Benefits

Administrative Manual

PROGRAM TO PREVENT, DETECT & MITIGATE IDENTITY THEFT

150

EFFECTIVE DATE: AUGUST 1, 2009

REVISION DATE:

PURPOSE: Ensure that the Office of Employee Benefits can identify and respond to activities that are possible indicators of identity theft with regard to information pertaining to an individual's participation in a plan or program offered by the Office of Employee Benefits

SCOPE: Employees of The University of Texas System

STATUTORY AND ADMINISTRATIVE REFERENCES:
16 CFR 681.1

1.0 BACKGROUND

The purpose of this rule is to create a written plan to detect, prevent and mitigate Identity Theft that is attempted or perpetrated with regard to Participants in plans or programs offered by the Office of Employee Benefits (OEB) in compliance with 16 CFR 681.1, "the Red Flags Rule" issued by the Federal Trade Commission pursuant to Section 114 and 315 of the Fair Credit Reporting Act (FACTA) which amended the Fair Credit Reporting Act (FCRA).

2.0 DEFINITIONS

Covered Account: Any account that OEB maintains to provide to an individual with goods and services under a plan or program in return for premium payments made by or on behalf of that individual. For purposes of this policy, an individual's Covered Account includes all of the various programs or plans offered by OEB in which the individual is a Participant and all of the information maintained by or on behalf of OEB pertaining to the Participant.

Identity Theft: Any use or attempt by an individual to use another person's individual identifying information to obtain a thing of value including: money; credit; items; or services, such as medical care coverage or benefits, to which the individual is not entitled.

Individual Identifying Information: Any information that may be used alone or with other information to identify an individual including, but not limited to: (1) name; social security number, date of birth, telephone/cell number, insurance policy or certificate numbers, alien

registration number, passport number, employer or taxpayer identification number, credit/debit/banking account numbers; or enrollment information; (2) claims information or personally identifiable health information; (3) unique biometric data such as fingerprint, voice print, retina or iris image or other unique physical representation; (4) unique electronic identification number; address or routing code; IP or other computer identifying address; or (5) telecommunication identifying information or other access device.

Institution: A University of Texas System institution, including UT System Administration, whose benefits-eligible Employees and Retired Employees, and the benefits-eligible dependents of such Employees and Retired Employees, are entitled to participate in program and plans offered by OEB.

Participant: An Employee, Retired Employee or Surviving Dependent individual who is a Participant in a plan or program offered by OEB and who is the holder of a Covered Account.

Red Flag: Suspicious patterns or practices, or specific activities that indicate the possibility that Identity Theft may occur or is occurring in connection with OEB's Covered Accounts.

3.0 FACTORS CONSIDERED IN THE DEVELOPMENT OF THIS POLICY

The Office of Employee Benefits (OEB) has experienced a minimal history of attempted or actual fraud or identity theft perpetrated on a Covered Account created or maintained by or on behalf of OEB for services, although it has always been the policy and practice to maintain the privacy and security of all information relating to OEB plan and program Participants that is maintained by or on behalf of OEB.

OEB recognizes that insurance coverage, and in particular health care coverage, has become an increasingly important and valuable commodity, and that subsequently information relating to insurance coverage such as member identification numbers, has increasingly become a target for fraud and identity theft. At the same time, OEB has a duty to ensure the availability of insurance services to benefits-eligible Employees, Retired Employees and their eligible Dependents in a timely and efficient manner. In addition, the Health Information Portability and Accessibility Act (HIPAA) and the HIPAA Privacy regulations place a duty on health plans to ensure that individuals have reasonably prompt access to their own personal health records.

Many of the services related to the programs and plans provided by OEB are provided by third party vendors that provide or administer the benefits and services available through OEB. Therefore, a great deal, if not most, of the transactions that occur regarding a Participant's Covered Account are conducted by these third party vendors, and the information collected and maintained about these transactions are held by the vendors on behalf of OEB.

Given the diverse nature of the plan and programs provided or administered by its third party vendors, OEB has determined that fraud and Identity Theft occurring at the vendor level is best controlled by the vendors. OEB will therefore continue to require by contract that all third party vendors that perform activities in connection with Covered Accounts have written policies and procedures in place designed to detect, prevent and mitigate the risk of fraud and Identity Theft with regard to Covered Accounts and shall provide regular reports to OEB regarding its fraud and Identity Theft and data security Programs, and as necessary require notification on incidents involving OEB program and plan data to OEB to ensure that OEB and/or a Participant can take

steps necessary to prevent or mitigate future Identity Theft in connection with a Covered Account that is not under the control of the third party vendor.

In addition, eligibility for enrollment in OEB plans and programs is based on an individual's status as an Employee or Retired Employee in an Institution or as a certain Dependent of an active or deceased Employee or Retired Employee. Determination of that status and the initial creation of a Covered Account with an individual is under the control of the individual Institutions with which the active, deceased or Retired Employees are associated, rather than OEB. OEB merely receives the data used to create these accounts from the Institutions. Therefore, suspicious activity concerning the creation of a Covered Account that would constitute a Red Flag would normally occur at the Institution and would not be capable of detection or prevention by OEB.

Accordingly, suspicious activity under the direct control of OEB that would constitute a Red Flag centers around existing Covered Account accounts and attempts to obtain or intercept identification cards, debit cards and identifying data involving a Participant in an OEB plan or program that could be used to impersonate a Participant in order to obtain benefits and services available through OEB.

With regard to information held or transmitted directly by OEB staff, OEB shall control the potential for fraud and Identity Theft by maintaining technical and physical safeguard with regard to data relating to Covered Accounts and by training staff to recognize the existence of Red Flags with regard to any transactions with or about a Participant, and to take responsive action when a Red Flag is detected or reported.

4.0 TECHNICAL AND PHYSICAL SAFEGUARDS

4.1 Technical Safeguards. OEB complies with U T System Administration INT 124, Information Resources Acceptable Use and Security Policy, at all times. All electronic transfers of OEB data are overseen and performed by OEB's own information technology (IT) staff. OEB's IT staff monitors the security of all of its internal plan and program related systems resources and takes all necessary actions to protect data from unauthorized access. OEB relies upon the UT System IT security office to provide network security and administrative software password security according to industry standards in order to protect non-public Participant data that is maintained by UT System outside of OEB. The UT System Administration's Office of Technology Information Services at UT System provides network security and administrative software password access security according to industry standards in order to protect non-public customer information that is stored on OEB desktop computers and other electronic devices storing non-public customer information. Offsite storage and information processing by third party vendors generally conforms to the same practices as onsite storage, and is safeguarded under the provisions for outside services provided via contract.

4.2 Physical Safeguards. OEB uses direct personal control or direct supervision to control access to and handling of all non-public customer information when the office is open.
All non-public information is maintained, stored, transmitted and otherwise handled under the direct personal control of an authorized employee of OEB . Non-public information is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. Conversations concerning non-public information are held in private. Papers with non-public information are mailed via official interagency mail, U.S. mail, or private mail

carrier. Electronic files of non-public information are encrypted when transmitted electronically. When best practices permit the disposal of non-public information, it is destroyed; paper containing such information is confidentially destroyed. The OEB offices have restricted access, cabinets or other locked storage areas. When offices are open, confidential information is kept out of sight from visitors, and computer screens are not visible to visitors. Offices and/or computers are locked when the office will be vacant for an extended length of time. After-hours access is limited to authorized employees with electronic pass cards. UT System security further ensures the security of offices after hours. OEB offsite storage and information processing by third party vendors generally conforms to the same practices as onsite storage, and is safeguarded under the provisions for outside services provided via contract.

5.0 VERIFICATION OF EMPLOYEE REQUESTS TO MAKE CHANGES TO EXISTING ACCOUNTS

All requests for changes to Covered Accounts are verified to have come from or as having been made by a Participant, an Institution's Benefits Office, or an authorized third party vendor.

5.1 Changes Made Through OEB or an Institution

OEB Staff and Institution Benefits Offices must verify the identity of each Participant who requests a change to an existing account, including a Participant's request to change a mailing address or for additional or replacement identification cards, as follows:

5.1.1. Changes Entered Online

a. OEB accepts online account changes directly from a Participant only though its secure system, MY UT Benefits, which requires Employees to enter a secure password or other secure authenticating information order to access the system.

b. OEB will accept change requests, including mailing address changes, from an Institution that were initiated by a Participant through an on line system, only if the system utilized by the Institution requires the Participant to enter a secure password or other authenticating code to make changes to their Covered Accounts.

5.1.2 Employee Submits Change Requests Via E-mail

a. OEB does not accept change requests directly from Participants via e-mail.

b. An Institution Benefits Office that by policy allows Employee's to make change requests via e-mail may accept change requests sent through institutional email if the Employee must use a secure Password to access their institutional e-mail program to send the e-mail form.

5.1.3 Employee Makes Change in Person

a. OEB does not accept in-person account changes from Participants.

b. An Employee who comes to an Institution's Benefits Office to make changes to an account, must be required to present a valid photo identification (e.g., Employee ID card, passport, or driver's license) for verification unless they are personally known to the Institution's staff member accepting the change request.

5.1.4 All Other Change Request Methods

An Institution that accepts change requests via a non-secure on-line process, telephone, mail, or via an e-mail request that does not come via an Employee's institutional password protected e-mail must verify that the request was made by the Participant by one of the following methods:

a. If the request is from an Employee using a non-secure, password protected Institutional e-mail account: E-mail the Employee using the Employee's secure, password protected Institutional e-mail address and receiving confirmation that the Employee requested the change via return e-mail from that secure e-mail account;

b . If the request is made via telephone: Require the requestor to verify his or her identity by providing secure information on file for that individual or to correctly answer a pre-selected security question;

c. For requests made using any method other than the methods described in Sections 5.1.1, 5.1.2, or 5.1.3, supra: Send a written notification of the change request to the mailing address that was on file for the Participant, prior to the receipt of the change request, which notification must contains clear and reasonable instructions for promptly report an incorrect change request, or

d. If an Institution has adopted other reasonable policies and procedures as part of an Institution's program to prevent, detect and mitigate Identity Theft (Idenity Theft Program) that include processes for validation of address change requests: Follow compliance with the institution Identity Theft Program.

5.1.5 Processing of Change Requests

a. Only change requests that have been verified as described in Sections 5.1.1, 5.1.2, 5.1.3, or 5.14, supra will be accepted by OEB .

b. OEB will send the changes to the vendor providing or administering the benefit plan on behalf of OEB via secure data transmission.

5.1.6 Identification of Red Flag and/or Receipt of Unverifiable Requests

a. An institution that receives a change request that is accompanied by a possible Red Flag or that is not verifiable for any reason should notify OEB and report and investigate the matter pursuant to the Institution's Identity Theft Program and/or fraud policies. The Institution shall promptly report the outcome of any such investigation to OEB.

b. Upon receipt of such a report, OEB will log the report, review the report and if warranted by the report, flag the Participant's account and notify third party vendors as appropriate. If OEB determines that the Red Flag indicates a likely attempt by an unauthorized third party to access a Participant's account information or divert a participant's mail, and the Institution has not done so, OEB may notify the Participant of the attempted access and/or the attempted change.

5.2 Changes Made Through an OEB Vendor

OEB shall contractually ensure that all vendors authorized by OEB to accept change requests from a Participant have reasonable policies and procedures in place to prevent, detect and mitigate Identity Theft. If the services provided by a vendor include acceptance of address changes or requests for new or additional identification or other cards associated with the account, the vendor's policies and procedures must include reasonable policies and procedures to verify the validity of a change request and a process for notifying OEB of unverifiable requests.

6.0 PARTICIPANTS' REQUESTS TO ACCESS TO CLAIMS DATA & OTHER PHI

Participants have a right to access their own claims data and other personal health information (PHI) that is subject to HIPAA pursuant to OEB's HIPAA Privacy Policies. These policies are located in the OEB Administrative Manual at Policy 400, "Health Insurance Portability and Accountability Act". The policies outline the methods to be used for responding to requests for such information by or on behalf of a Participant for access to PHI, including verification requirements.

7.0 RED FLAGS

The following have been identified as potential Red Flags based on the Risk Factors associated with OEB's Covered Accounts:

- Any unusual or suspicious activity related to Covered Accounts
- A report that a Participant's secure password, PIN or other authenticating item has been lost, stolen, or otherwise compromised
- An unverifiable request to change a Participant's mailing address
- Receipt of documents in support of creation of an account, change to an existing account change or a claim for benefit or services that appear to be forged, altered, to identify a person other than the individual one whose behalf the document is presented or otherwise suspicious
- Notification from a Participant, law enforcement, service provider or third party vendors of unusual activity related to a Covered Account
- Notification from a credit bureau of fraudulent activity regarding a Covered Account
- A complaint or question from an Account Holder based on the Account Holder's receipt of:
    - a bill for another individual
    - a bill for a product or service that the Participant denies receiving
    - a bill from a health care provider that the Participant denies patronizing; or
    - a notice of health plan benefits or other third party payor payments made on behalf of a Participant (such as an Explanation of Benefits) for health services the Participant never received.
- Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the Participant
- A Participant or third party vendor report that plan or program coverage is denied because benefits have been depleted or a lifetime cap has been reached
- A dispute of a bill or Explanation of Benefits by a Participant who claims to be the victim of any type of Identity Theft
- A notice or inquiry from an insurance fraud investigator for a private insurance company or a state or federal regulatory or law enforcement agency
- A statement from a Participant that a plan or program identification card, debit card, bill; or explanation of benefits was requested but never received

8.0 MITIGATION

An OEB employee who encounters or receives a report from an Institution or third party vendor about the existence of a Red Flag or who otherwise becomes aware of possible activity that indicates potential or existing fraud or Identity Theft with regard to a Covered Account shall notify his or her supervisor and the Director of OEB or the Director's designee ("the Responsible Individual."). Upon receipt of such a report, the Responsible Individual will log the report and gather all available information regarding the transaction, and ensure that any or all of the following actions are taken as applicable:

- Notification of all applicable OEB employees, Institution Benefits Offices and third party vendors that there may be a problem with the Covered Account and/or placing an alert in applicable records that Identity Theft is believed to be occurring or have occurred with regard to the Participant's Covered Account
- Contacting UT System Office of Police or other law enforcement agencies upon discovery of possible Identity Theft in connection with a Covered Account
- Ensuring that any passwords, PINs, or other authenticating codes that have been compromised relating to the Covered Account are changed
- Notifying the Participant of the possible or actual Identity Theft in situations where notification is necessary to or likely to permit the Participant to take action to protect him or herself from the consequences of the Identity Theft
- Correcting erroneous information in the Covered Account record resulting from actual or attempted fraud or Identity Theft
- Conducting File extraction—purging the Participant's file to the extent possible of all information that was entered as a result of the fraudulent activity, and replacing with a brief cross-reference and explanation of the deletion. The purged information is then placed into a new file
- Determining that no response is warranted under the particular circumstances.
- Taking any other action determined by the OEB Director or the Director's designee to be reasonable under the circumstances to prevent or mitigate Identity Theft with regard to the Covered Account

9.0 DOCUMENTATION

OEB will document all reports of actual or potential Identity Theft and their outcomes for use in periodic evaluation of this Policy.

10.0 REVIEW AND EVALUATION OF PLAN AND RED FLAGS

OEB will review this Policy no less than annually and revise it to reflect changes in operations and changes in potential risks of Identity Theft.

11.00 TRAINING

OEB will ensure that all employees are aware of this Identity Theft Detection Policy and receive training on all changes made to this Policy.

Effective Date: August 1, 2009