VII. STANDING COMMITTEES

B. Finance, Audit and Facilities Committee

Adoption of University of Washington "Red Flag" Policies

RECOMMENDED ACTION:

It is the recommendation of the administration and the Finance, Audit and Facilities Committee that the Board of Regents approve the University of Washington's policies regarding identity theft in compliance with the Federal Trade Commission's Red Flag Rules, as set forth below.

BACKGROUND:

The Federal Trade Commission (FTC), in November 2007, issued what is known as the "Red Flag Rules," requiring certain entities (financial institutions which provide accounts covered by the rules) to implement internal policies to help identify and prevent identity theft. Within the University, examples of applicable activities include the Federal Perkins Loan Program, offerings of plans for payment of tuition throughout the quarter, and payment arrangements with patients for health care services.

University administration has developed an institutional policy as prescribed by the FTC's Red Flag Rules; UW Medicine has developed a specific policy governing patient accounts. The University policy is attached and will be incorporated into the University's Administrative Policy Statements; the UW Medicine policy is also attached and will be incorporated into the UW Medicine Compliance Policy Statements.

FTC's rules require approval of these policies by the Board of Regents. As noted in the policies, University administration will provide periodic reports on the Red Flag programs implementation and administration to the Finance, Audit and Facilities committee, in accordance with the FTC requirements.

REVIEW AND APPROVALS

This recommendation has been approved by the Senior Vice President for Finance and Facilities and the CEO of UW Medicine, Executive Vice President for Medical Affairs, and Dean of the School of Medicine.

Attachments

1. Administrative Policy Statement 35.2 – Identity Theft Prevention: Red Flag Rules
2. UW Medicine Identity Theft Prevention Program Policy

Identity Theft Prevention: Red Flag Rules

(Approved by the Senior Vice President for Finance and Facilities by authority of Executive Order No. 5 and the CEO of UW Medicine, Executive Vice President for Medical Affairs, and Dean of the School of Medicine by Executive Order No. 6)

1. Purpose and Scope

In its capacity as a creditor, the University of Washington (UW) is subject to 16 CFR 681 [http://www.access.gpo.gov/nara/cfr/waisidx_09/16cfr681_09.html], "Identity Theft Rules," which requires the establishment of a written Identity Theft Prevention Program for covered accounts (defined below). To protect existing consumers, reduce risk from identity fraud, and minimize potential damage from fraudulent new accounts with the least possible impact on business operations, the University establishes this Identity Theft Prevention Program (hereafter, the program). The program policies and guidelines apply to UW entities, departments, and employees when conducting business activity relating to UW covered accounts. Additional policies and procedures may be imposed by UW entities that have unique types of covered accounts.

2. Definitions

Covered Account: A consumer account that the University offers or maintains primarily for personal purposes and that involves multiple payments for goods or services provided by the University, or any other account for which there is a reasonably foreseeable risk of identity theft. Covered accounts may include, but are not limited to, tuition receivables, student loans and collections, and patient billing.

Identity Theft: Fraud committed using the identifying information of another person.

Personally Identifiable Information: An individual's first name and last name and at least one of the following data elements: social security number, driver's license number or identification card number, account number, credit card number, debit card number, security code, access code, or password of an individual's covered account.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

3. Policy

It is the policy of the University to:

- Identify covered accounts.
- Verify identification for any student, faculty member, staff member, or patient requesting services. The identification should be scrutinized to verify that it has not been altered or forged.
- Verify that the picture and physical description on the identification provided matches the appearance of the customer presenting the identification.

- Verify that the information on the identification is consistent with other information on file at the University, particularly information on the customer's account.
- Verify that requests for information updates have not been altered or forged, or that the paperwork does not give the appearance of having been destroyed and reassembled.
- Decline to share with a customer any more information than what is documented in the student system if there is a full Family Educational Rights and Privacy Act (FERPA) restriction [http://www.washington.edu/students/reg/ferpafac.html] on the account.
- Investigate and verify the correctness of unauthorized charges or transactions assessed in connection with a customer's account.
- Require UW entities, units, and/or departments that are responsible for a significant number or unique type of covered accounts (such as patient accounts in healthcare entities) to establish additional policies and procedures for detecting and responding to red flags.
- Include standard contractual language requiring entities that provide services associated with covered accounts to have policies and procedures to detect, prevent, and mitigate the risk of identity theft.
- Use due diligence to form a reasonable belief, when a notice of address discrepancy is received from a consumer reporting agency, that the information relates to the individual for whom the original request was submitted. In developing this belief, the UW entity will:

  #1 Compare information received from the consumer/credit reporting agency with entity records (registration changes, change of address notifications, account information, etc.).

  #2 Contact the student, faculty member, staff member, or patient to verify their address.

  #3 Use other reasonable means to verify that the correct address is associated with the student, faculty member, staff member, or patient and consumer report.
- Promptly provide the correct address, after establishing a reasonable belief that the correct address is known, to the reporting agency that issued the notification of address discrepancy.
- Recognize that the issuing of credit plays an important role in this University program. The UW currently **does not issue** credit/debit cards. However, the University **does accept** credit and debit cards.
- Continue meeting the requirements of the Gramm-Leach-Bliley Act (GLBA) Policy [https://www.washington.edu/admin/finacct/office/glb/glbprog.html].
- Continue meeting the requirements of the Health Insurance Portability and Accountability Act (HIPAA) privacy [http://depts.washington.edu/comply/privacy.shtml] and security [http://depts.washington.edu/comply/security.shtml] policies.
- Continue meeting the requirements of the Emergency Medical Treatment and Active Labor Act (EMTALA), per 42 USC Section 1395dd.

4. Identification and Detection of Red Flags

The UW recognizes that the following types of notices, documents, personal information, and activities may be indicators or red flags that an individual's identity may be compromised:

a. Alerts, Notifications, or Warnings from a Consumer Reporting Agency

#1 A fraud or credit alert is included with a consumer report.

#2 A notice of credit freeze on a consumer report is provided from a consumer reporting agency.

#3 A consumer report agency provides a notice of address discrepancy.

#4 A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a customer.

b. Suspicious Documents

#1 Documents provided for identification appear to have been altered or forged.

#2 The photograph and/or physical description on the identification is not consistent with the appearance of the customer presenting the identification.

#3 Other information on the identification is not consistent with information provided by the person opening an account or presenting the identification.

#4 Other information on the identification is not consistent with readily accessible information that is on file with the University.

#5 An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

c. Suspicious Personal Identifying Information

#1 Personal identifying information provided is not consistent with external information sources used by the University.

#2 Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.

#3 Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University.

#4 The social security number provided is the same as that submitted by other persons opening an account or other customers.

#5 The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or to other customers.

#6 The person opening the account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

#7 Personal identifying information provided is not consistent with personal identifying information that is on file with the University.

#8 If the University uses a challenge question, the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

d. Unusual Use of, or Suspicious Activity Related to, the Covered Account

#1 Shortly following the notice of a change of address, the University is made aware of a new cell phone number or the addition of authorized users on the account.

#2 A new revolving credit account is used in a manner commonly associated with known patterns of fraud.

#3 An account is used in a manner that is not consistent with established patterns of activity on the account.

#4 An account that has been inactive for a reasonably lengthy period of time is used.

#5 Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account.

#6 The University is notified of unauthorized charges or transactions in connection with a customer's account.

e. Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts

The University is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that a fraudulent account has been opened.

f. Compromised Systems

Detection of compromised or breached systems that store covered accounts or personally identifiable information.

g. Additional Red Flags

The University recognizes that additional red flags may be identified by UW entities, units, and/or departments for specific types of covered accounts.

5. Responding to Red Flags

The University will respond appropriately to identified and detected red flags in order to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed.

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the University from damages and loss.

Approved standards and responsive action must be maintained by each unit based upon business and technical needs. The University recommends the following responses to red flags:

- Alert and involve a business unit manager;

- Notify designated University official;
- Monitor a covered account for evidence of identity theft;
- Where appropriate, change any passwords, security codes, or other security devices;
- Close an existing covered account;
- Reopen a covered account with a new account number if needed;
- Contact customer;
- Request additional documentation to validate identity;
- Handle per regulatory requirements under law if applicable;
- Handle per applicable University privacy and information security policies, as noted in Section 3;
- Notify law enforcement or regulatory entity; or
- Determine no response is warranted under the particular circumstances.

6. Administration of the Program

a. Board Approval of Written Program

The UW Board of Regents adopted the program on July 16, 2009.

b. Designation of University Official

The UW has designated the Senior Vice President for Finance and Facilities, and, for UW Medicine, the CEO of UW Medicine, Executive Vice President for Medical Affairs, and Dean of the School of Medicine, to be the program's two institutional officials. These officials are responsible for implementing program policies; seeing that entity-specific procedures are established; assigning responsibility for investigating and responding to red flags; periodically reassessing entity operations to verify where covered accounts are opened and maintained; recommending program modifications as needed; generating periodic status reports; and reporting annually to the Board of Regents' Finance, Audit, and Facilities Committee on the effectiveness of the UW Identity Theft Prevention Program.

c. Training

The University will train all employees, officials, and contractors for whom contact with covered accounts is reasonably foreseeable. Training will also be provided as changes to the program are made. Training will include operating procedures for identifying and detecting identity theft as well as responding to identity theft.

d. Security Practices of Contractors and Service Providers

The UW expects all third party contractors and service providers who handle covered accounts to follow and be compliant with all federal, state, and local laws or regulations that are applicable to the University, as well as University policies and procedures that are relevant to the underlying contract between the parties. The specific terms and issues of such compliance are addressed in the University contractual documents.

e. Reporting Requirements

Annual reporting requirements will be presented to the Board of Regents' Finance, Audit, and Facilities Committee.

7. Additional Information

For related policies, see:

- APS 2.1 [http://www.washington.edu/admin/rules/APS/02.01TOC.html], "UW Information Systems Security"
- UW Medicine Identity Theft Prevention Program Policies 1-6 [http://depts.washington.edu/comply/policies.shtml]

For additional information, contact one of the following offices:

Student Fiscal Services
- Phone: 206–685–7671
- Fax: 206–616–2678
- Campus mail: Box 355870
- Email: cashmgmt@u.washington.edu

UW Medicine Compliance
- Phone: 206–616–5248
- Fax: 206–221–5172
- Campus mail: Box 358049
- Email: comply@u.washington.edu

ITPP Policy Number: 1 Effective Date: August 1, 2009

PROGRAM COMPONENTS

Background

The University of Washington (UW) is subject to 16 CFR Part 681 "Identity Theft Rules". Section 16 CFR 681.2 imposes specific duties regarding the detection, prevention, and mitigation of identity theft on Creditors, including non-profit organizations and government entities that maintain Covered Accounts, including the requirement to develop and implement a written Identity Theft Prevention Program (ITPP). The UW Guidelines for Preventing, Detecting and Mitigating Identity Theft set forth the University level ITPP (UW ITTP) and apply to all University Covered Accounts.

UW Medicine entities collect registration and billing information to create Patient Accounts and/or bill for the provision of healthcare services. Patient Accounts are a specific subset of Covered Accounts. UW Medicine has established a specific ITPP for this specific subset of Covered Accounts.

Purpose and Scope

The following policy statements establish the UW Medicine Identity Theft Prevention Program (UW Medicine ITPP) for new and existing patient accounts, and articulate key responsibilities for program oversight and implementation. These policies apply to UW Medicine entities[1] and their workforce members.

Definitions

Covered Account: An account that a creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or any other account for which there is a reasonably foreseeable risk from identity theft.

Creditor: Any entity that regularly extends, renews, or continues credit or any entity that regularly arranges for the extension, renewal, or continuation of credit.

Identity Theft: Fraud committed using the identifying information of another person.

Patient Account: For purposes of the UW Medicine ITPP, Patient Account means a Covered Account that is offered or maintained by a UW Medicine entity for a patient in connection with the provision of healthcare services.

[1] UW Medical Center, Harborview Medical Center, Airlift Northwest, UW Physicians (UWP), UW Medicine Neighborhood Clinics/UW Physicians Network (UWPN), UW School of Medicine

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Policy Statements

1. UW Medicine will maintain and administer an Identity Theft Prevention Program (ITPP) in order to detect, prevent, and mitigate identity theft in connection with new or existing patient accounts.

2. The initial UW Medicine ITPP will be approved by the UW Board of Regents. The UW Medicine Board Compliance Committee will receive periodic assessments of the effectiveness of the UW Medicine ITTP.

3. Each UW Medicine entity will:

    a. Participate in periodic assessments of the UW Medicine ITPP to determine if program modifications are necessary.
    b. Engage in periodic assessments of entity-specific procedures and activities to evaluate compliance with the UW Medicine ITPP and verify program effectiveness.
    c. Report related activities at least annually to the CEO of UW Medicine, Executive Vice President for Medical Affairs, and Dean of the School of Medicine or his designee.

4. The UW Medicine ITPP includes the following components:

    a. Risk Assessment (see 5b below).
    b. Internal safeguards to prevent and mitigate identity theft (UW Medicine ITPP Policies 2 & 4).
    c. A list of relevant red flags for patient accounts (UW Medicine ITPP Policy 3).
    d. Recommended procedures to be followed when red flags are detected (UW Medicine ITPP Policies 3, 4, 5, 6).
    e. Standard contract language requiring entities that provide services associated with patient accounts to have policies and procedures to detect, prevent and mitigate the risk of identity theft.

5. Roles and responsibilities associated with the oversight, implementation and management of the UW Medicine ITPP include the following:

    a. The Designated Official (DO) for the UW Medicine ITPP is the CEO of UW Medicine, Executive Vice President for Medical Affairs, and Dean of the School of Medicine. The DO delegates the Associate Vice President for Medical Affairs/Chief Compliance and Privacy Officer with responsibility for overseeing development and maintenance of the UW Medicine ITPP; establishing requirements and timelines for entity status reports; coordinating system-wide assessments and case management for issues involving multiple entities; updating the program as needed; and preparing a system-wide status report.

b. Each entity will designate an individual to oversee its implementation of UW Medicine ITPP policies; establish entity-specific procedures to ensure compliance; assign responsibility for investigating and responding to red flags; periodically reassess entity operations to verify where patient accounts are opened and maintained; recommend program modifications as needed; and generate periodic status reports. This designation will be established in consultation with the UW Medicine ITPP DO (see 5a above), and communicated in writing to appropriate entity officials and workforce members.

c. Each entity's Compliance Office oversees the development and delivery of UW Medicine ITPP training to its workforce members.

d. All UW Medicine workforce members are responsible for adhering to established policies and implementing procedural safeguards.

6. UW Medicine will adhere to the UW Guidelines for Preventing, Detecting and Mitigating Identify Theft for other types of covered accounts that may exist. Where appropriate, the UW Medicine ITPP incorporates safeguards established by the UW Guidelines.

References

16 CFR 681: Identity Theft Rules (http://www.access.gpo.gov/nara/cfr/waisidx_08/16cfr681_08.html)

Associated Policies and Procedures

- UW Guidelines for Preventing, Detecting and Mitigating Identify Theft
- HMC Policy 135.17, Patient Identification Clarification Process