Boonshoft School of Medicine
WRIGHT STATE UNIVERSITY

Name: Red Flag Policy

Created: 05/17/2010 Revised: 07/03/17, 06/30/2015, 09/07/2011

References:

Wright State Policy 9610 – Identity Theft Prevention Program

Federal Trade Commission – The Red Flags Rules

Purpose:

The purpose of this policy is to identify specific Red Flag areas within the medical school and apply the Wright State Policy to them. While this policy will target specific areas for Red Flag, all personnel should treat all data sensitively and according to any pertinent regulations.

Covered Accounts:

Covered Accounts are found in AMCAS, Atlas, BAMS, Banner, Flight, ExamSoft, MedSIS, and New Innovations. With regards to Clinical Software programs, those items are covered under the policies established at Wright State Physicians.

Step 1 - Identifying relevant red flags:

Red Flag means a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Some categories of red flags are:

- Alerts, notifications or others warnings received from consumer reporting agencies or service providers
- The presentation of suspicious documents
- The presentation of suspicious personal identifying information
- The unusual use of or other suspicious activity related to a Covered Account

Step 2 - Detecting red flags:

Student account creation – Medical student applicants apply to AMCAS and are verified at that level. Students accepted here have the AMCAS data electronically transferred to Banner. This creation process should contain minimal risk.

Visiting Students – Visiting student information is verified by the home school, regardless of whether the student is using VSAS or not.

Transfer Students – Information should be compared to the verified data in AMCAS. The student will be required to provide appropriate picture identification in order to receive a Wright1 card.

Faculty/Staff account creation – Some accounts are created for faculty and staff. The guidelines established by the General Person/Process (GPP) FACT and Human Resources (HR) should be followed for data entry. SSN should not be entered unless the person will be a WSU employee.

Resident account creation – Prospective residents apply to ERAS and are verified at that level. ERAS data is electronically transferred to Banner. This creation process should contain minimal risk. Residency coordinators should electronically transfer data from ERAS to New Innovations to minimize risk.

Alumni account creation – Alumni accounts should never be created. These accounts will be created when the alumni started as a student.

Donor account creation – Donor account creation is handled by University Advancement. Data submitted to the University should be verified.

Account updates – Regardless if data updates are keyed directly or submitted to the University, all information should be verified according to University policy (Wright State Policy 9610).

Information requests – All requests for information should be handled carefully. Release of information should follow University policy (Wright State Policy 9610). For cases of account owners verifying information, please confirm the identity of the account owner. Request the current information and compare to the system, rather than giving the owner the information.

Sensitive academic records – This information is covered by a variety of legislation and policies (Security Policies). This information should also be considered for possible identity theft.

Step 3 - Responding to red flags:

Any suspected red flag activity should be reported immediately. Please report to the person responsible for the system below. When in doubt, contact the Associate Dean for Fiscal Affairs.

AMCAS, New Innovations – Associate Dean for Student Affairs/Admissions
Atlas, Flight. ExamSoft – Manager, Medical Academic Operations
Banner – Executive Director and CFO
BAMS, MedSIS – SAA Business Services Manager

If a red flag is verified, the above responsible person should report it to both CaTS and the Executive Director and CFO. CaTS reporting is available online.

Step 4 - Administering the program:

Responsibility for developing, implementing and updating this Program lies with the Executive Director and CFO. The Administrator will be responsible for annual review of the policy, ensuring appropriate training of identified individuals, reviewing reports of red flag detection and establishing steps to prevent identity theft.