IDENTITY THEFT PREVENTION PROGRAM – RED FLAG RULES

I. Purpose

New York Medical College (the "College") has developed this identity theft program (the "Program") pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 to detect, prevent and mitigate identity theft at the College in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program.

II. Scope

The Program includes reasonable procedures to:

1. Identify relevant red flags for covered accounts the College offers or maintains and incorporate those red flags into the Program.
2. Detect red flags that have been incorporated into the Program.
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
4. Ensure the Program is updated periodically to reflect changes in risks to students and employees or to the safety and soundness of the creditor from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

III. Definitions

A. Identity Theft

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 risk of identity theft.

C. Covered Account

An account that the College offers or maintains, primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include but are not limited to student account/loan information, credit/debit card processing, financial aid information, checking and savings accounts, payroll account information and any other account that the College offers or maintains where there is a reasonable foreseeable risk to individuals or to the safety and soundness of New York Medical

College from identity theft, including financial, operational, compliance, reputation or litigation risks.

IV. Policy

It is the policy of New York Medical College to detect, prevent and mitigate identity theft at the College in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program.

V. Identification of Relevant Red Flags

In order to identify relevant Red Flags, the College considers the types of accounts that 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 are relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

A) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

B) The presentation of suspicious identification or other documents such as those appearing altered or forged or inconsistent with existing information of the College;

C) The presentation of suspicious personal identifying information, such as a photograph or physical description that is not consistent with the appearance of the individual presenting the identification or inconsistent with information previously provided to or on file with the College such as birth dates, addresses;

D) The presentation of identifying information that is the same as information shown or found to be fraudulent or that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

E) A request made from a non-College issued e-mail account;

F) A request to mail something to an address not listed on file;

G) The unusual use of, or other suspicious activity related to a covered account; or

H) Notice from students, employees, victims of identity theft, credit bureau, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

VI. Response

The Program shall provide for appropriate responses to detect red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

A) Deny access to the covered account until other information is available to eliminate the Red Flag;

B) Notify the Senior Vice President for Finance and Chief Financial Officer and the Vice President and General Counsel of the red flag activity;

C) Contact the individual whose account may have been compromised;

D) Change any passwords, security codes or other security devices that permit access to a covered account;

E) Notify law enforcement; or

F) Determine that no response is warranted under the particular circumstances and eliminate the red flag.

VII. Updating the Program

The Program shall be periodically updated to reflect changes in risks associated with covered accounts or to the soundness of the College from identity theft related to the noted covered accounts based on factors such as:

A) The College's experience with identity theft;

B) Changes in identity theft methods;

C) Changes in identity theft detection and prevention;

D) Changes in the types of accounts the College offers or maintains; and

E) Changes in the College's business arrangements with other organizations.

After considering these factors, the Senior Vice President for Finance and Chief Financial Officer shall determine whether changes to the Program, including the listing of red flags, are warranted. If warranted, the Program will be updated.

VIII. Program Oversight

The Senior Vice President for Finance and Chief Financial Officer of the College shall have the responsibility for developing, implementing and updating this Program. Such responsibilities shall include program administration, ensuring appropriate training of the College's staff on the

Program, reviewing any staff reports regarding the detection of red flags on the identified covered accounts and the steps for preventing and mitigating Identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

IX. Staff Training

College staff responsible for implementing the Program shall be trained in the detection of red flags, and the responsive steps to be taken when a Red Flag is detected.

Approved by the Finance Committee of the Board of Trustees on August 12, 2009 and by the Board of Trustees on December 16, 2009.