OFFICE OF COMPLIANCE
IDENTITY THEFT PROGRAM

I. POLICY

Eastern Virginia Medical School (EVMS) establishes the following identity theft program ("Program") to detect, identify, and mitigate identity theft in its Covered Accounts in accordance with the Fair and Accurate Credit Transactions Act (FACTA) of 2003 and its "Red Flag Rules."

II. DEFINITIONS

Covered Accounts: Any account EVMS offers or maintains that involves multiple payments or transactions, or any other accounts where EVMS collects or maintains sensitive information as defined below that, if acquired by an unauthorized party, could result in Identity Theft. Examples of Covered Accounts include: student admissions applications, student financial records, employee personnel and payroll files, transcripts and academic files, and vendor information.

Covered Areas: Those EVMS departments that have activities with Covered Accounts.

Identifying Information: Information that may be used, alone or in conjunction with other information, to identify a specific person such as: name, address, telephone number, Social Security Number (SSN), date of birth, maiden name, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or employee or student identification number. Directory information as defined by the EVMS Family Educational Rights and Privacy Act (FERPA) Annual Notice for Students is excluded from this definition.

Identity Theft: A fraud committed using the Identifying Information of another person.

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

Sensitive Information: Privileged documents or information, whether stored in electronic or printed format, which if compromised through unauthorized access, could reveal Identifying Information and encourage or result in Identity Theft, such as: credit card account number (in part or whole) and cardholder name or address; tax returns, W-2's, 1099's, or other tax documents; paychecks, pay stubs, direct deposit information or other payroll information; admissions records and transcripts; and medical information including doctor names, insurance information or claims, prescription information and any related personal medical information.

III. IDENTIFICATION OF RED FLAGS

The following are Red Flags:

A. Notifications and warnings from credit reporting agencies such as:

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an individual or applicant;
3. Notice or report from a credit agency of an address discrepancy for an applicant; or
4. Indication from a credit report of activity that is inconsistent with an individual's usual pattern or activity, such as a recent and significant increase in the volume of inquiries; an unusual number of recently established credit relationships; a material change in the use of credit, especially with respect to recently established credit relationships; or an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. Suspicious documents such as:

1. Identification document or card that appear to be forged, altered, or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other information on the identification is not consistent with readily accessible information that is on file such as a signature card or a recent check; or
4. Application for service that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious personal identifying information such as:

1. Personal identifying information provided that is inconsistent when compared against external information sources used by EVMS. For example: an address that does not match any address in the consumer report; a SSN has not been issued, or is listed on the Social Security Administration's Death Master File;
2. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by the individual. For example, there is a lack of correlation between the SSN range and date of birth;
3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by EVMS. For example:

the address on an application is fictitious, a mail drop, or prison; the phone number is invalid, or is associated with a pager or answering service;

4. The SSN provided is the same as that submitted by other persons opening an account or other individuals;
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 other individuals;
6. The person opening the covered account or the individual 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 EVMS; or
8. For applications that use challenge questions, the person opening the covered account or the individual 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, a Covered Account, such as:

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to EVMS that an individual is not receiving mail sent by EVMS;
6. Notice to EVMS that an account has unauthorized activity;
7. Phone calls to EVMS asking to verify employment for individuals who are no longer active employees at EVMS or who are employees leaving EVMS.

E. Breach or attempted breach of any aspect of EVMS' computer system security; and

F. Notice to EVMS from a student, employee, Identity Theft victim, law enforcement or other persons that EVMS, or an individual employed by EVMS, has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. PRACTICES FOR DETECTING RED FLAGS

A. New Accounts. In order to detect any of the Red Flags identified above associated with the opening of a new account, personnel in Covered Areas should take the following steps to obtain and verify the identity of the person opening the account:

1. Ensure that the application or record submitted is authentic and does not appear to have been altered;
2. Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;
3. Verify the individual's identity by reviewing a driver's license or other identification card; and
4. Review any additional documentation provided by the individual or a third-party (credit reporting agency, prior employer, and prior school) for discrepancies.

B. Existing Accounts. In order to detect any of the Red Flags identified above for an existing account, personnel in Covered Areas should take the following actions:

1. Verify the identification of individuals if they request information whether in person, via telephone, via facsimile or via email and require the use of secure login software where available;
2. Verify the validity of requests to change billing or other addresses; and
3. Verify changes in banking information given for billing and payment purposes.

C. The Office of Compliance and each Covered Area will, as necessary, develop and implement specific methods and protocols for opening and monitoring Covered Accounts in those Covered Areas with specific or substantial need.

V. MITIGATING IDENTITY THEFT/RESPONDING TO RED FLAGS

A. Personnel in Covered Areas shall take the following steps to mitigate Identity Theft:

1. Storage space containing documents with Identifying Information and/or Sensitive Information must be locked or secured when not in use;
2. Work areas, printers and fax machines must be cleared of all documents containing Identifying Information and/or Sensitive Information when not in use;
3. Complex passwords will be used, if possible, for any program that stores Identifying and/or Sensitive Information;
4. All emails sent or received that contain Identifying Information and/or Sensitive Information must be printed and deleted, saved to the network or moved to personal folders, but should not remain in the recipients email Inbox. In addition, any

Identifying Information and/or Sensitive Information sent externally must be encrypted and password protected and sent only to approved recipients;

5. When documents containing Sensitive Information are discarded they must be placed inside a locked shred bin or shredded using a mechanical cross cut or other high security shredding device; and
6. From time to time, each Covered Area that utilizes or transmits Identifying Information in databases, email, on documents or by other methodology, must review the Identifying Information used and determine if such information is crucial for the Covered Area to meet its mission. Particular attention should be paid to the use and transmission of SSN information, which should only be an identifier when absolutely necessary.

B. All incidents involving Red Flags or Identity Theft will be thoroughly investigated. Personnel in Covered Areas who detect Red Flags, or otherwise suspect Identity Theft must immediately contact the EVMS Police Department, 757-446-5911, and/or the Office of Compliance, 757-446-6008. In the event that any ensuing investigation requires the disclosure of information maintained by the EVMS Information Technology (IT) Department, the request for such information must be made by the EVMS Office of the General Counsel or Human Resources.

C. In the event of an actual or potential electronic security breach from an outside source such as a hacker, phishing email, lost laptop or other circumstances with the potential for Identity Theft, the following steps shall be taken.

1. The IT Department shall, as soon as practicable, report the breach to the user of the electronic device or system, and the EVMS Office of Compliance. EVMS IT shall also begin containment and mitigation procedures as necessary, which may include: locking affected user out of network services temporarily, capturing current state of compromised services for a user, restoring compromised services for a user, reviewing compromised services for a user for risk of data loss, user credential changes, user education, firewall rule changes and internet access changes.
2. Within 5 business days of the breach, the IT Department shall determine the scope of the breach and begin efforts to restore data, if possible. Information about the breach will be made available to the EVMS Office of Compliance, who will notify other affected persons or entities as necessary.
3. The EVMS Office of Compliance will require breached users to complete a Risk Assessment Form that details any personal/identifiable information relating to patients, students, staff or confidential EVMS operations that may have been contained on the electronic device or system, or affirmation that no risk of data loss

existed. Notification may also include instructions to complete technology security training. The disclosure must contain certification language and the user's signature. Responses will be shared with EVMS Risk Management, IT, EVMS Medical Group Compliance, and other affected entities as necessary for follow-up.

4. Within 14 business days of the breach, the IT Department shall provide the Office of Compliance with a brief report that outlines the circumstances surrounding the breach.
5. The EVMS Medical Group Compliance will handle any required notification of affected individuals for data breaches related to patients. The EVMS Office of Compliance will handle any required notification of data breaches related to students, staff, and institutional operations.

D. All EVMS personnel in Covered Areas shall make volunteers, non-compensated employees, and service providers and contractors performing work for Covered Areas, aware of this Program and how to detect, mitigate and respond to Red Flags. A service provider or contractor that maintains its own Identity Theft prevention program, consistent with the guidance of the Red Flag Rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

VI. SANCTIONS

Any EVMS employee who is found to have improperly accessed or utilized the Identifying Information of another individual, whether that person is known to them (i.e. family or friends) or not, may be subject to immediate termination in accordance with EVMS Disciplinary Action Policy.

VII. IDENTITY THEFT PROGRAM ADMINISTRATION AND MANAGEMENT

A. The Program is effective as of June 1, 2010 and shall be administered by the EVMS Office of Compliance. The Office of Compliance is responsible for identifying Covered Areas and developing, implementing, and updating the Program including appropriate training, reviewing reports regarding the detection of Red Flags, and providing assistance as needed to Covered Areas in determining which steps of prevention, response and/or mitigation to take in particular circumstances.

B. The Program will be periodically reviewed and updated to reflect changes in Identity Theft risks and technological changes.