POLICY/PROCEDURE NO.: B-26
Effective date: May 1, 2009
Date(s) of revision: _____

Policies and Procedures:
IDENTITY THEFT PREVENTION

Section: **Compliance**
Chapter: **Administration**
Policy: **Identity Theft Prevention**

I. PURPOSE

The purpose of this policy is to protect patients and West Virginia University Physicians of Charleston (WVUPC) from loss caused by identity theft and to assure the integrity and accuracy of medical records in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

II. APPLICABILITY

This policy applies to all WVUPC employees and to all individuals/entities entering into contracts to do business with WVUPC.

III.

WVUPC has established an Identity Theft Prevention Program (Program) to detect, prevent and mitigate identity theft in connection with patient accounts and patient medical records. The Program includes reasonable policies and procedures to:

- Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
- Detect red flags that have been incorporated into the Program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

The Program incorporates existing WVUPC policies and procedures that control reasonably foreseeable risks.

WVUPC, through this program, requires that all contracted service providers implement reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft if they perform activities with WVUPC patient accounts or medical records.

IV. PROCEDURE

ADMINISTRATION OF PROGRAM:

Security Team: The WVUPC Board of Directors designates a Security Team to oversee this program which will consist of at least the following individuals (or their designees):

- Security Officer
- Privacy Officer
- CFO
- Compliance Officer
- VP, Human Resources
- CIO

Administration: The CIO, with the assistance of the Security Team, shall be responsible for the development, implementation, oversight and continued administration of the Program.

- The Security Team shall coordinate an annual review of the Identity Theft Prevention Program. During the review process, the Security Team will evaluate the results of the periodic reviews and follow-up procedures, to determine whether revisions or additions are necessary.
- The Security Team shall provide oversight for training of staff, as necessary, to effectively implement the Program; and
- The Security Team shall exercise appropriate and effective oversight of service provider arrangements.

Population Covered

All WVUPC employees, providers, volunteers, contractors and vendors

Responsible Persons

All WVUPC employees, providers, volunteers, contractors and vendors

Definitions

Identity Theft: means fraud committed or attempted using the identifying information of another person without authority. The information can be used to falsely obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. Within this policy, identity theft includes medical identity theft.

Medical Identity Theft: Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity – such as insurance information or Social Security Number – without the victim's knowledge or consent to obtain medical services or goods, or when someone uses the person's identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.

Procedures

Identify Red Flags: A **red flag** is any action or event which:

- Provides an unauthorized person with access to and/or ability to use, disclose, modify or destroy Protected Information; or
- Permits an unauthorized person to modify systems, including any equipment or device and any software application or operating system which is a component of an Information System; or
- Permits a software application which is not authorized under the Acceptable Use policy to access or perform actions affecting Protected Information or the functioning of any Information System or component of an Information System.

*Common examples of Red Flags can be found in **Addendum 1** attached hereto.*

Detecting Red Flags: In order to detect potential identity theft, WVUPC shall request the following information at time of registration:

- Driver's license, passport, or other photo identification (if available)
- Social Security Number
- Date of birth
- Residence address and telephone number
- Insurance card (if available)

Actions to take based on the Red Flag encountered.

- Re-validate the identifying information with the patient
- Ask for another form of identification
- Alert the care provider of possible John or Jane Doe
- Create a new account and/or medical record
- Initiate an investigation
- Ask for help from your supervisor or manager

Reporting Red Flags:

- All WVUPC employees, providers, volunteers, contractors and vendors will report suspicious activity to an immediate supervisor or a member of the Security Team.
- The supervisor will report the Red Flag to a member of the Security Team promptly.
- The Security Team shall conduct the investigation in accordance with the procedures set forth in *Addendum 2, attached hereto.*

Responding to complaints of identity theft and mitigating actual cases of theft: If an individual claims to be a victim of identity theft, WVUPC will investigate the claim by asking the individual to complete one of the following documents:

1. The ID Theft Affidavit developed by the Federal Trade Commission, including supporting documentation; or
2. A written statement including the following information:
    - A statement that the individual is a victim of identity theft
    - A copy of the individual's driver's license or identification card

- Any other identification document that supports the statement of identity theft
- Specific facts supporting the claim of identity theft, if available
- Any other explanation that the individual did not incur the debt
- Any available correspondence disputing the debt
- Documentation of the residence of the individual at the date of service, including copies of utility bills, tax statements, or other statements from business sent to the individual at his/her residence
- A telephone number for contacting the individual
- Any information that the individual may have concerning the person who registered in their name.
- A statement that the individual did not authorize the use of his/her name or personal information for obtaining services
- A statement certifying that the representations are true, correct, and contain no material omissions of fact to the best knowledge and belief of the person submitting the certification.

Mitigate: If, following an investigation, the Security Team concludes that the individual has been a victim of identity theft, WVUPC will take the following actions:

1. WVUPC will cease collection on open accounts that resulted from the identity theft. If the accounts were referred to collection agencies, the collection agencies will be instructed to cease collection activity.
2. WVUPC will cooperate with any law enforcement investigation relating to the identity theft to the extent allowed by law.
3. If an insurance company, government program or other payor has made payment on the account, WVUPC will notify the payor and refund the amount paid.
4. WVUPC will contact medical staff and contracted care/service providers involved in the care of that patient so that refunds and collection activities can be addressed by those departments/individuals as well.

If following an investigation, it does not appear that the individual has been a victim of identity theft, WVUPC or the collection agency will give written notice to the individual that he/she is responsible for payment of the bill (if any). The notice will state the basis for determining that the person claiming to be a victim of identity theft was in fact the patient.

Handling of medical records in cases of identity theft:

- If it is confirmed that a patient record was created as the result of identity theft, a notation concerning the identity theft will be placed in the record. All demographic information will be removed from the record.
- The Health Information Management Department will determine whether any other records are linked to the record found to be created through identity theft.
- In some cases, identity theft may involve an identity thief receiving care under the name of another person, who has been a patient. In such a case, the

patient's file will be reviewed and any information relating to the identity thief will be removed and segregated.

- WVUPC will contact medical staff and contracted care/service providers involved in the care of that patient so that medical record amendments/corrections can be addressed by those departments/individuals as well.

Education of Staff Regarding Identity Theft: Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to WVUPC or its customers.

Duties Regarding Address Discrepancies

If WVUPC receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report, WVUPC may reasonably confirm that an address is accurate by any of the following means:

- Verification of the address with the consumer;
- Review of the records;
- Verification of the address through third-party sources; or
- Other reasonable means.

If an accurate address is confirmed, WVUPC shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

- WVUPC establishes a continuing relationship with the consumer; and
- WVUPC, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

Regulatory Requirement

Fair Credit Reporting Act (commonly referred to as "FCRA"), 15 U.S.C. §1681m
Fair and Credit Transactions Act of 2003 (commonly referred to as "FACT Act"), Pub. L. No. 108-159, §114, 117 Stat. 1960 – 1961.
Identity Theft Rules, 16 C.F.R. §681.2, 15 C.F.R. Pt. 681, App. A (2008).

Addendum 1: Red Flag examples.

Addendum 2: Red Flag investigation procedures

POLICY/PROCEDURE NO.: B-26
Effective date: May 1, 2009
Date(s) of revision: _____

ADDENDUM 1

Red Flag examples

Critical Incidents:

- Employee theft of Protected Information
- Disruption of or denial of service of critical systems, including clinical decision-support applications, financial reporting systems, and electronic medical records information
- Unauthorized access to security administrator applications or information
- Unauthorized access to Protected Information requiring unprivileged or public notification of affected third-party individuals

Moderate Incidents:

- Employee views of medical record of fellow employees without authorization
- Worm causes fraudulent mass emailing from infected systems.

Minor Incidents:

- "Phishing" email is received
- Employee accessing prohibited websites

Suspicious Activity

- Access logs show a limited number of unsuccessful attempts by an authorized user
- Employee loiters near restricted work area beyond his authorization
- User returns to workstation to find new application started without initiation.

The following Red flags/Security Incidents are potential indicators of fraud:

- Alerts, notifications or warnings from a consumer reporting agency;
- A fraud or active duty alert included with a consumer report;
- A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
- A notice of address discrepancy from a consumer reporting agency as defined in §334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

Consumer reports: Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, 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.

Suspicious documents:

- Documents provided for identification that appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with WVUPC, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious personal identifying information:

1. Personal identifying information provided is inconsistent when compared against external information sources used by WVUPC. For example:
   - The address does not match any address in the consumer report;
   - The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
   - Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
   - The photograph on a driver's license or other photo ID card submitted by the patient does not resemble the patient.
   - The patient's signature does not match a signature on file in WVUPC's records.
   - The Social Security Number or other identifying information furnished by the patient is the same as identifying information in WVUPC's records furnished by another individual.
2. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by WVUPC. For example:
   - The address on an application is the same as the address provided on a fraudulent application.
   - The address on an application is fictitious, a mail drop, or a prison; or
   - The phone number is invalid or is associated with a pager or answering service.
3. The SSN provided is the same as that submitted by other persons opening an account or other customers.

4. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.
5. The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
6. When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
7. A patient reports to a scheduler phoning a patient to remind them of an appointment that they did not make an appointment.

Unusual use of, or suspicious activity related to, the covered account.

1. Shortly following the notice of a change of address for a covered account, WVUPC receives a request for new or additional information.
2. Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's covered account.
3. WVUPC is notified that the patient is not receiving paper account statements.
4. WVUPC receives notice from patients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by WVUPC.
5. WVUPC is notified by a patient, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
6. The patient calls to report that they received an explanation of benefits from their insurance company for an encounter that they did not have.

ADDENDUM 2

Red Flag investigation procedures

The investigation should address the following:

1. Patient medical records – hospital, clinic, home health, lab
2. Patient accounting systems - hospital, clinic, home health, retail pharmacy, other ancillary services providers
3. Service Recovery – if the patient or a member of the community initiates the notification
4. Security Officer – audit trail of access to information systems
5. Security – if there is a concern regarding patient or staff safety
6. Clinical – flag chart as potential medical identity theft

All reports of potential or suspected Security Incidents shall be documented upon receipt.

Upon receipt of information indicating the possible occurrence of a Red Flag, the Security Team shall:

- Assign a preliminary rank to the Red Flag; and
- Designate an Incident Leader from the Security Team for each Red Flag.

The **Incident Leader** will investigate any such report appropriately, including follow up interviews and log and audit trail reviews. The Incident Leader will be responsible for identifying and coordinating responsive actions; identifying and convening the members of the Team necessary or appropriate for response to the incident; coordinating with the Legal Department, Public Affairs and other internal parties; and reporting the incident and responses to the Team and the Board of Directors.

The **Security Team** will be responsible for reviewing audit trails and logs throughout the Information Systems. Such reviews will be conducted with respect to a given device or application whenever a Security Incident or Suspicious Activities are reported which may involve unauthorized access to the device or application.

The **Security Team** shall consult promptly with the WVUPC General Counsel to determine whether the Security Incident may expose WVUPC to material legal penalties and/or liabilities. If there appears to be a material risk of such penalties or liabilities, the Security Team shall promptly consult with General Counsel to determine whether the investigation and reporting should be conducted through or under the oversight of legal counsel. External consultants, technical experts and/or legal counsel may be retained for purposes of incident response.

Any actions taken in response to a potential or suspected Security Incident shall be documented. The originals of all Security Incident documentation shall be kept by the Security Team.

V. Amendment or Termination of this Policy

This policy may be amended or terminated at any time.

VI. References

- Insert legal citations if applicable.