THREE RIVERS DISTRICT HEALTH DEPARTMENT

Detection and Prevention of Identity Theft

Policy A-IC-25

November 1, 2009

Purpose: These policies for the prevention and detection of identity theft and medical identify theft are intended to comply with the requirements of the federal Identity Theft Red Flags and Address Discrepancies Final Rule ("Red Flags Rule") that the Federal Trade Commission promulgated under the Fair and Accurate Credit Transactions Act of 2003 ("The FACT Act"). They are designed to comply with the requirements of the Red Flags Rule.

In all instances, these policies shall be interpreted and construed consistent with the requirements of the Red Flags Rule. In the event of any conflict between a provision of these policies and a requirement of the Red Flags Rule, the Red Flags Rule requirement shall control.

Policy: All of the policies contained or referred to in these privacy policies, or that may be added or otherwise established by Three Rivers District Health Department in the future, represent policies established by Three Rivers District Health Department for the members of its workforce in relation to the particular subject addressed by the policy. It is the intention of Three Rivers District Health Department that its employees and other members of its workforce use the Red Flags Rules policies in meeting their responsibilities to Three Rivers District Health Department. Violation of a policy can be the basis for discipline or termination of employment; however, because these policies relate to the establishment and maintenance of high standards of performance, under no circumstances shall any policy be interpreted or construed as establishing a minimum standard, or any evidence of a minimum standard, of the safety, due care, or any other obligation which may be owed Three Rivers District Health Department, its employees, or its agents to another person.

Procedure: All employees are subject to and required to comply and be familiar with the Detection and Prevention of Identity Theft regulations, policies and procedures as identified below:

I. Definitions
   A. Account. As used in these policies, the term "account" means a continuing relationship established by a person with Three Rivers District Health Department to obtain a product or service for personal, family, household, or business purposes. [16 C.F.R. § 681.1(b)(1)]
   B. Creditor. As used in these policies, the term "creditor" means Three Rivers District Health Department.

C. Covered account. As used in these policies, the term "covered account" means any account Three Rivers District Health Department maintains primarily for personal or household purpose that allows a patient or financially responsible party to make multiple payments for services. The term also applies to any other account that Three Rivers District Health Department for which there is a reasonably foreseeable risk to customers or to the safety and soundness of Three Rivers District Health Department form identity theft. Covered accounts maintained by Three Rivers District Health Department include Environmental, Home Health Services, and Clinic Services.

D. Electronic protected health information or EPHI. As used in these policies, the term "electronic protected health information" or "EPHI" has the same meaning as in Three Rivers District Health Department HIPAA Security Rule Policies and Procedures.

E. Identifying information. As used in these policies, the term "identifying information" means any name or number that may be used, alone or in conjunction with any other information to identify a specific person including, but not limited to, any:
    1. Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
    2. Unique biometric data, such as fingerprint, voiceprint, retina or iris image, or other unique physical representation.
    3. Unique electronic identification number, address, or routing code;
    4. Telecommunication identifying information or access device; or
    5. Health insurance account numbers; policy information, or other insurance information.

F. Red Flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

II. Duties of Compliance Officer.

A. Approval. After developing the original Identity Theft Detection and Prevention Program the Identity Theft Officer shall obtain the approval of the program from Three Rivers District Health Department District Board of Health. This shall be documented in writing by resolution of the District Board of Health and documented in the minutes of the board meeting at which the policies were approved.

B. Training. The Compliance Officer shall provide training to Three Rivers District Health Department staff regarding Three Rivers District Health Department Identity Theft Detection and Prevention policies and procedures.

C. Reporting. The Compliance Officer reports directly to Three Rivers District Health Department District Board of Health. The Compliance Officer shall report to Three Rivers District Health Department District Board of Health when policies/procedures have changed regarding Three Rivers District Health Department compliance efforts. This report should include the following information:
    1. The purpose of the program changes;

2. Significant incidents involving identify theft and management's response thereto; and
3. Recommendations for further changes to the program.

III. Training. All members of Three Rivers District Health Department workforce shall be trained at least annually on Three Rivers District Health Department policies and procedures with respect to identity theft prevention and detection as necessary and appropriate for the members of the workforce to carry out their functions within Three Rivers District Health Department.

A. Each member of the workforce on November 1, 2009, shall be trained by no later than November 1, 2009. Thereafter, each new member of the workforce shall be trained within thirty (30) calendar days after the person joins the workforce. Each member of the workforce whose functions are affected by a material change in these privacy policies or procedures shall be trained at the next quarterly staff meeting after the material change becomes effective.
B. Documentation of the training for each member of the workforce shall be kept in written or electronic form for six (6) years after the date of its creation or the date that a person ceases to be a member of Three Rivers District Health Department workforce, whichever is later.

IV. Identifying relevant red flags

A. Identifying covered accounts – at least annually, the Compliance Officer shall review the type of accounts Three Rivers District Health Department maintains in order to update Three Rivers District Health Department's list of covered accounts. This shall be incorporated into the annual HIPPA subcommittee annual review.
B. Annual assessment – At least annually, the Compliance Officer shall evaluate the Red Flags that are relevant to Three Rivers District Health Department's covered accounts. This review shall be incorporated into the annual HIPPA subcommittee annual review.
C. Risk factors – When performing the assessment, the Compliance Officer shall consider the following factors:
    1. The types of Covered Accounts Three Rivers District Health Department maintains;
    2. The methods Three Rivers District Health Department provides to open its covered accounts;
    3. The methods Three Rivers District Health Department provides to access its covered accounts; and,
    4. Three Rivers District Health Department's previous experience with identity theft.
D. Sources of red flags. When performing the assessment, the Compliance Officer shall also consider the following sources of Red Flags:
    1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
    2. Presentation of suspicious documents by a client, beneficiary, financially responsible party, etc.;

3. Presentation of suspicious identifying information, such as a suspicious address change;
4. The unusual use of, or suspicious activity related to, a covered account;
5. Discrepancies in the client's medical record and/or discrepancies between the client's medical record and (i) the medical history provided by the patient/client, (ii) information learned from the assessment; and,
6. Notice from a client, a victim of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Three Rivers District Health Department's covered accounts.

E. Examples of red flags.
   1. Admission red flags
      a. Discrepancies in Client Information.
      b. Suspicious identifying or other documentation.
   2. Red flags related to existing patients
      a. Security incidents. Any security incident, as that term is defined in Three Rivers District Health Department's Privacy and Security Policies and Procedures is a Red Flag.
      b. Unauthorized disclosure of PHI. Any unauthorized disclosure of PHI or EPHI is a Red Flag.
      c. Client complaint about a bill or explanation of benefits. When a client calls to inquire about a bill or an explanation of benefits they have received, this may be simply due to a client's failure to understand the bill or EOB they have received. This may also be due to identify theft. All such calls shall be treated as Red Flags.
      d. Notice of exhaustion of benefits. A notice that Medicare, Medicaid, or other insurance will no longer cover a client's care may be due to the legitimate exhaustion of benefits. It may also be an indicator that the client is the victim of identity theft. Any such Notices should be treated as Red Flags.

V. Detecting red flags.
   A. Upon admission/creation of new covered accounts. The following procedures shall be followed to identify Red Flags during the client admission process.
      1. Upon referral. When Three Rivers District Health Department receives a referral for a new client, Three Rivers District Health Department shall verify client identity by obtaining appropriate identification and insurance information. This shall include the following:
         a. Full name;
         b. Date of birth;
         c. Government issued photo identification;
         d. Insurance card, Medicare Card, etc.,
      2. Whenever possible, the patient's information shall be verified with the insurance provider and with the referral source.
      3. During admission. Three Rivers District Health Department admits a new client, Three Rivers District Health Department staff completing

admission paperwork or performing an admission assessment shall be on alert for:

a. Medical conditions listed by the client that are not reflected in the clients medical record or medical conditions listed in the clients medical record that the client does not mention as part of their medical history;
b. Prior treatments, procedures, or similar medical care that is listed in the client's medical record, but that is not evidenced during a routine examination of the client, for example, the client's medical record mentions a prior surgery, but the client does not have a scar are Red Flags. Similarly, evidence of prior treatments, procedures, or previous medical care that is not in evidence in the client's medical record should be considered a Red Flag. For example, during the assessment, the nurse notices a scar from surgery that is not reflected on the client's medical records.
c. Family members calling the client by a different name.

B. Existing client covered accounts. The following procedures shall be followed to detect Red Flags in relation to existing client covered accounts.
    1. Security incidents. These should be addressed pursuant to Three Rivers District Health Department's HIPAA Security Rule Policies and Procedures. If it is determined that the Security Incident may lead to Identity Theft, Three Rivers District Health Department shall respond according to these procedures on Preventing and Mitigating Identity Theft.
    2. Unauthorized disclosures of PHI. These should be addressed pursuant to Three Rivers District Health Department's privacy rule policies and procedures. If it is determined that Unauthorized Disclosure may reasonably lead to identity theft, Three Rivers District Health Department shall respond according to these procedures on Preventing and Mitigating Identity Theft.
    3. Complaint regarding a bill or explanation of benefits. If Three Rivers District Health Department's billing department or other staff members receive a complaint from an individual regarding a bill that has been received or an Explanation of Benefits, Three Rivers District Health Department shall treat this as a Red Flag.
    4. Request for an accounting of disclosures of PHI, request to access Phi, and/or request to amend PHI. This may be an effort by a victim of identity theft to fix damage done by an identity thief.
    5. Lost or stolen laptops and/or client files. When a staff member of Three Rivers District Health Department notifies Three Rivers District Health Department that he/she has lost files, had files stolen, lost a laptop or otherwise lost client information, Three Rivers District Health Department shall treat this as a Red Flag.
    6. Allegation by Client that Client is the victim of Identity Theft. When a client contact Three Rivers District Health Department and alleges he/she is the victim of Identity Theft, this is a Red Flag. Three Rivers District Health Department shall inform the client they should report the identity

theft to law enforcement. The client should be provided a copy of the FTC Identify Theft Affidavit to complete and submit. A copy of this affidavit shall be placed in the client's file. Three Rivers District Health Department shall follow up as required.

VI. Responding to red flag situations

A. Responding to red flags. Whenever the Compliance Officer receives notification that a member of Three Rivers District Health Department's staff has detected a red flag, the Compliance Officer shall respond in a manner that is commensurate with the risk posed by the Red Flag that has been detected. In evaluating an appropriate response, the Compliance Officer shall consider aggravating factors that may heighten the risk of identity theft.

B. Investigating. The first step in responding to a red flag is determining whether identity theft has occurred, might occur, or whether the red lag may simply be ignored. In order to make this determination, the Compliance Officer or an individual designated by the Compliance Officer must investigate the Reported Red Flag. The investigation shall be intended to identify such factors as:
    1. Whether the red flag indicator that identity theft has already occurred or might lead to identity theft.
    2. Whether Three Rivers District Health Department is dealing with the individual or the identity theft.
    3. Whether Three Rivers District Health Department has received any reimbursement for services provided to someone other than the beneficiary.
    4. Whether the red flag requires any response.

C. Any actions taken to respond to a Red Flag in an effort to prevent Identity Theft from occurring should be documented by the Compliance Officer and filed in the Administrative filing system. This documentation shall be maintained for six (6) years from date of occurrence.
    1. Prevention and Mitigation. When Three Rivers District Health Department's response to a Red Flag determines that identity theft has occurred, or might reasonably occur, Three Rivers District Health Department shall take steps reasonably designed to mitigate the damage caused by the identity theft. These steps may include:
        a. Notifying the individual who is the victim of the identity theft (this may not be the agency's client);
        b. Notify law enforcement of the identity theft;
        c. Notify other healthcare providers who have received PHI regarding the individual;
        d. Notify Medicare, Medicaid, or private insurers of the identity theft;
        e. Amend records to remove false information, as appropriate;
        f. Not admitting a client where the investigation determines the putative client is an identity thief;
        g. Cease attempting efforts to collect payments from an individual when it is determined the individual is the victim of identity theft

and was not the person who received the services from Three Rivers District Health Department;

h. If federally reimbursable services were provided due to identity theft committed by the party receiving the services, notify the appropriate fraud enforcement authorities, identify the amount received for these services and repay them; or
i. Any other actions designed to mitigate the damage done by the occurrence of identity theft.

D. HIPAA and red flags. Three Rivers District Health Department has implemented policies and procedures designed to comply with the requirements of the HIPAA Privacy and Security Regulations. Any actions taken to investigate a red flag, prevent identity theft or to mitigate identity theft shall be done in compliance with these policies and procedures.

VII. Review and update policies and procedures

A. Review of policies and procedures.
   1. Annual review. At least annually, Three Rivers District Health Department's compliance officer shall review Three Rivers District Health Department's Identity Theft policies and procedures for the Identification and Prevention of Identity Theft. This review shall reflect changes in risks to patients from identity theft or to the safety or soundness of Three Rivers District Health Department from identity theft. This review shall performed during the annual HIPPA subcommittee review and shall be based upon factors including but not limited to:
      a. Three Rivers District Health Department's experience with identity theft;
      b. Changes in methods of identity theft;
      c. Changes in methods to detect, prevent, and mitigate identity theft;
      d. Changes in the types of accounts Three Rivers District Health Department offers or maintains; and
      e. Change in the business arrangements of Three Rivers District Health Department including mergers, acquisitions, alliances, joint ventures, and services provider agreements.
   2. Review other than annually. If a new Red Flag is identified, or Three Rivers District Health Department experiences an incident of Identity Theft, Three Rivers District Health Department's Compliance Officer shall review Three Rivers District Health Department's Identity Theft Policies and Procedures in order to evaluate whether this experience requires any revisions or modifications of Three Rivers District Health Department's identity theft policies and procedures.

B. Revising policies and procedures. After performing a review as required by these Policies and Procedures, if Three Rivers District Health Department's Compliance Officer determines Three Rivers District Health Department's Identity Theft Policies and Procedures are no longer reasonable and appropriate to (1) the size and complexity of Three Rivers District Health Department or (2) the nature and scope of Three Rivers District Health Department's activities, Three

Rivers District Health Department's Compliance Officer shall revise them accordingly.

1. Documentation. Three Rivers District Health Department's Compliance Officer shall document the annual or other review that was performed, the conclusions of that review, and the changes that were made as a result.
2. Revisions. All revisions to the Policies and Procedures shall be in writing and approved in writing by the board. The Compliance Officer will meet with the board to discuss any proposed changes to the Policies and Procedures.
3. Training. The Compliance Officer shall arrange for training for the members of Three Rivers District Health Department's staff regarding any new policies and procedures at the next quarterly staff meeting of the revisions to the Policies and Procedures.

District Director **Date**

Chairperson, Three Rivers District Board of Health **Date**