Creation Date: 10/29/2013
Revision Date: 10/29/2013
Approval Date: 12/18/2013
Revision: A

Identity Theft Prevention Program (ITPP) – Red Flag Rules

1. Purpose

a. Clark County's policy is to protect customers and their accounts from identity theft by detecting, preventing, and mitigating identity theft as required by the Fair and Accurate Credit Transaction Act of 2003 (FACTA) and the Federal Trade Commission (FTC) Red Flags Rules, 16 C.F.R. §681.

b. This ITPP addresses the following:
   i. identifying relevant identity theft Red Flags;
   ii. detecting those Red Flags;
   iii. responding appropriately to any that are detected to prevent and mitigate identity theft; and
   iv. updating our ITPP periodically to reflect changes in risks.

c. Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

2. Definitions

a. Covered Account: An account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. A covered accounts also includes an account for which there is a foreseeable risk of identity theft.

b. Creditor: An individual or entity subject to Fair Credit Report Act who provides covered accounts (i.e. allowing multiple payments or transactions), and defers payments (i.e. postponing payments to a future date and/or installments payments).

c. Employee: Any agent, employee, officer, or official of the county who provides services in connection with a covered account.

d. Identifying Information: Any name or number that may be used to identify a specific person, including: name, address, telephone number, social security number, date of birth, driver's license number, employee identification number.

e. Identify Theft: Fraud committed using the identifying information of another person.

f. Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

g. Service Provider: Any person or entity that provides a service directly to the county that is related to a covered account.

3. Scope

a. This ITPP applies to covered accounts that are maintained by a county department and service providers that perform activities in connection with our covered accounts under a county contract.

4. **Risk Assessment**
   - **a.** Based on the nature of these covered accounts and the presence of other privacy protecting mechanisms (i.e. HIPAA), the risk of identity theft is low.

5. **ITPP Approval and Administration**
   - **a.** Clark County's Board of Supervisors is responsible for the approval of this ITTP. The Clark County Corporation Counsel is designated as identity theft officer and is responsible for the oversight, development, training, and administration of this ITPP.

6. **Identification of Red Flags**
   - **a.** To identify relevant identity theft Red Flags, Clark County assesses various risk factors, including:
     - **i.** the types of covered accounts;
     - **ii.** the methods used to create these accounts;
     - **iii.** the methods used to access these accounts; and
     - **iv.** previous experience with identity theft.
   - **b.** Clark County also considers the sources of Red Flags, including identity theft incidents Clark County has experienced; addressing likely identity theft techniques; and changing applicable supervisory guidance.
   - **c.** In addition, Clark County considers Red Flags from the following four (4) categories, in addition to the 26 numbered examples from Supplement A to Appendix A of the FTC's Red Flags Rule:
     - **i.** suspicious documents;
     - **ii.** suspicious personal identifying information;
     - **iii.** suspicious account activity; and
     - **iv.** notices from other sources.
   - **d.** Refer to Appendix A for identified Red Flags.

7. **Detection, Prevention, and/or Mitigation of Red Flags**
   - **a.** Each county employee or service provider handling a covered account is required to be alert for any notice from a customer, victim of identity theft, law enforcement authorities, or other business regarding possible identity theft in connection with a covered account held by the county.
   - **b.** Upon receipt of such a notice, the employee or service provider is required to promptly report the red flag to his/her departmental head, who will then promptly report the Red Flag to the Corporation Counsel.
   - **c.** Refer to Appendix A for suggested techniques/steps for detecting, preventing, and/or mitigating the different types of identified Red Flags.

8. **Responses to Red Flags**
   - **a.** Corporation Counsel will review each reported Red Flag to determine the following:
     - **i.** the appropriate level of investigation required with the assistance of the appropriate department head and/or employee;
     - **ii.** if the county's insurance company needs to be contacted; and

iii. the appropriate response based on the nature of the Red Flag.

b. The appropriate response may include any of the following:

i. Monitor a covered account;
ii. Contact the customer;
iii. Suspend a covered account;
iv. Deny the opening of a covered account;
v. Close a covered account;
vi. Reopen a covered account with a new account number;
vii. Review similar covered accounts;
viii. Notify law enforcement; and/or
ix. Not respond.

9. Internal Compliance Reporting

a. Corporation Counsel will report at least annually to the Clark County Executive Committee regarding the effectiveness of the ITPP in addressing the risks of identity theft in connection with covered accounts, service provider arrangements, significant incidents involving identity theft, responses, and/or recommendations for changes to the ITPP if deemed necessary.

b. Inquiries regarding Clark County's ITPP may be directed to:

Office of Corporation Counsel
Clark County Courthouse
517 Court Street
Neillsville, WI 54456
(715) 743-5223

APPENDIX A – Identified Red Flags and Detection/Protection Activities

1. Clark County maintains few covered accounts, including, but not limited to:
    a. billing and collection related to medical services;
    b. billing and collection for community mental health/developmental disabilities/alcoholism/drug abuse services;
    c. treasurer's agreement with taxpayer for payment of delinquent property taxes by installments;
    d. clerk of circuit court's establishment of payment plans, unpaid fines, forfeitures, and other payments ordered by the court;
    e. sheriff department's maintaining of inmate funds; and
    f. receipt of deposits and payment of bills for client accounts).
2. Clark County has identified the following Red Flags:
    a. Red Flags for documents, such as:
        i. Documents provided for identification that appear to be forged or altered;
        ii. Documentation on which a person's photograph or physical description is not consistent with the person presenting the documentation;
        iii. Documentation with information that is not consistent with existing customer information; and/or
        iv. Application for service that appears to have been altered or forged.
    b. Red Flags for personal identifying information, such as:
        i. Individual identifying information is inconsistent with other information that the customer provides;
        ii. Individual's identifying information is the same as shown on other applications found to be fraudulent;
        iii. Individual's identifying information is consistent with fraudulent activity;
        iv. Individual's Social Security number ("SSN") is the same as another patient/customer's SSN;
        v. Individual's address or phone number is the same as that of another person;
        vi. Individuals fails to provide complete personal identifying information on an application when asked to do so; and/or
        vii. Individual's identifying information is not consistent with the information that is on file for the patient/customer.
    c. Red Flags for activity related to an account, such as:
        i. Change of address for an account followed by a request to change the account holder's name;
        ii. Account being used in a way that is not consistent with prior use;
        iii. Mail sent to the account holder is repeatedly returned as undeliverable;
        iv. Clark County receives notice that a customer is not receiving paper statements;

v. Clark County receives notice that an account has unauthorized activity;
vi. Clark County receives notice that an account has activity that is inconsistent with a patient/consumer's usual pattern or activity;
vii. Clark County receives a complaint from a patient/consumer based on the patient/consumer's receipt of:
    1. Bill for another individual.
    2. Bill for a product or service that the consumer denies receiving.
    3. Bill from a health care provider that the consumer never patronized.
    4. Notice of insurance benefits (or explanation of benefits) for health care services never received.
viii. Records showing medical treatment that is inconsistent with a physical examination or with medical history as reported by the patient;
ix. Complaint or question from a patient/consumer about the receipt of a collection notice;
x. Patient/Consumer or health insurer report that coverage for items or services is denied because insurance benefits have been depleted or a lifetime cap has been reached;
xi. Dispute about a bill by a consumer who claims to be the victim of identity theft; and/or
xii. Patient who has an insurance number but never produces an insurance card or other documentation of insurance.

3. Clark County complies with state and federal regulations that require that each component of Clark County be diligent in detecting any of the Red Flags identified above in connection with the opening of a new account and to take the following steps, as appropriate, to obtain and verify the identity of the person opening a new account:
    a. Verify an individual's identity by reviewing and, if necessary, copying a driver's license or other identification card.;
    b. Review documentation showing the existence of a business entity; and/or
    c. Require, as applicable, the name, date of birth, residential or business address, principal place of business for an entity, and Social Security number, tax identification number, driver's license information, or other identification.
4. In order to detect and prevent any of the Red Flags identified above, Clark County's component personnel should be trained to take the following steps to monitor transactions involving such accounts:
    a. Compare presented documents to other similarly situated valid document;
    b. Ask for clarification on unclear information provided on document;
    c. Have document reviewed by multiple individuals;
    d. Verify documentation is complete and original;
    e. Store documentation within secure location;
    f. Destroy documentation after intended use and appropriate retention period;
    g. Ensure all requested information is provided or accounted for;
    h. Collect the minimal amount of information necessary;
    i. Redact personal information on Open Records requests;
    j. Review account activity for inconsistency or abnormally large transactions;

k. Confirm suspicious activity with client; and/or
l. Verify account authorization.