To: Associate

From: Jennifer Eubanks, Compliance Officer

Please read the attached, answer the following questions and return to Carol Allen.

1. The purpose of the program is to:
    a. Identify the relevant Red Flags based on the risk factors associated with clinic covered accounts;
    b. Institute policies and procedures for detecting Red Flags;
    c. Identify steps RCI will take to respond to, prevent and mitigate Identity theft;
    d. Create a system for regular updates and administrative oversight of the Program.
    e. All of the above

2. The program applies to:
    a. The doctors and administrators only
    b. All employees including providers, administrators and staff
    c. Only the staff
    d. Only the patients
    e. None of the above

3. The risk for RCI is high because we receive most of our information from the hospitals. True or False

4. What are the Red Flags that are most relevant to RCI.
    a. Suspicious Documents
    b. Suspicious Personal Identifying Information
    c. Suspicious or Unusual Use of a Covered Account
    d. Alerts from Others
    e. All of the above

5. RCI will use its best efforts to assure that Identify Theft is not occurring by collecting and verifying information on existing and return patients. True or False.

6. If a red flag is detected by an employee of RCI should gather all documentation rand report the incident to the Compliance officer who is _____.

7. If the activity is determined to be fraudulent, name one action that RCI may take:

    _____

Signed: _____ Date: _____

RED FLAG IDENTITY THEFT DETECTION & PREVENTION POLICIES AND PROCEDURES
Radiology Consultants of Iowa, PLC
May 1, 2009

In compliance with the Federal Trade Commission's Identity Theft Prevention Red flags Ruling (16 CFR 681.2) the following policies and procedures have been developed, reviewed and approved by the Board of Managers of Radiology Consultants of Iowa, PLC (RCI). These policies and procedures have been created to expand on existing HIPPA Privacy and Security Rules to prevent unauthorized disclosure of protected health information. Preventing unauthorized access to and/or disclosure of patient information is critical to protecting patients from identity theft.

Note: Providing identification is not a condition for obtaining emergency care.

Program Purposes: The purpose of the program and attached policies are to:

1. Identify the relevant Red Flags based on the risk factors associated with clinic covered accounts;
2. Institute policies and procedures for detecting Red Flags;
3. Identify steps RCI will take to respond to, prevent and mitigate Identity Theft;
4. Create a system for regular updates and administrative oversight to the Program.

Scope: The program applies to all employees including providers, administrators and staff.

Definitions: For purposes of the program, the following terms are defined as:

- "Covered Account" means any account that a clinic maintains involving multiple payments or transactions, including one or more deferred payments.
- "Identity Theft" means fraud committed using the identifying information of another person.
- "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Risk Assessment
Identifying threats that could harm and, thus adversely affect compliance with rules and regulations applicable to RCI are an essential part of the Red Flag program. Risk assessment organizational policies and procedures as well as technical or physical controls are in place to mitigate risk. Registration, billing and coding and other identified personnel may be periodically interviewed by clinic management to assess possible risk factors. (See Exhibit A)

Physical safeguards of patient information are currently in place including password protected computer access, locked file cabinets and restricted visitor access. Proper disposal of patient identifying information will continue under this program.

Identification of Red Flags
The Identity Theft Red Flags Mitigation and Resolution Procedures (Exhibit B) identify the Red Flags that would be most relevant to RCI. These generally fall within one of the following general types of Red Flags:

1. Suspicious Documents
2. Suspicious Personal Identifying Information
3. Suspicious or Unusual Use of a Covered Account
4. Alerts from Others

Detection of Red Flags

RCI will use its best efforts to assure that Identity Theft is not occurring by collecting and verifying information on existing and returning patients. In order to facilitate detection of the Red Flags identified in Exhibit B, registration and reception staff will take the following steps to obtain and verify the identity of the person.

A. New Patients/Accounts
   1. Require identifying information (for example: full name, drivers license, DOB, address, government issued ID, other photo ID, Social Security card, insurance card, etc).
   2. If patient doesn't present insurance information, consider verifying coverage with insurance company.

B. Existing Accounts
   1. Verify validity of requests for changes of billing address, or any other patient demographic information.
   2. Verify identification of patient before giving out personal information.

Program Oversight & Reporting

The Company Compliance Officer is responsible for developing, implementing, administering and updating the Program. The Compliance Officer will be responsible for conducting an annual review & assessment of the policies and report the findings to the governing body. The Compliance Officer is responsible for assuring that all staff receive training. In the case where an employee of RCI has committed or participated in identity theft, existing disciplinary policies will be engaged.

If a red flag is detected by an employee of RCI:

1. The employee should gather all documentation and report the incident to the Compliance Officer.
2. The Compliance Officer will determine if the activity is fraudulent or authentic.
3. If the activity is determined to be fraudulent, then RCI should take immediate action. Actions may include:
   a. Cancel the transaction
   b. Notify the affected patient
   c. Notify the affected physician
   d. Notify appropriate law enforcement
   e. Assess impact to practice

If a patient claims to be a victim of identity theft, the patient should be encouraged to file a police report for Identity Theft if he/she has not done so already.

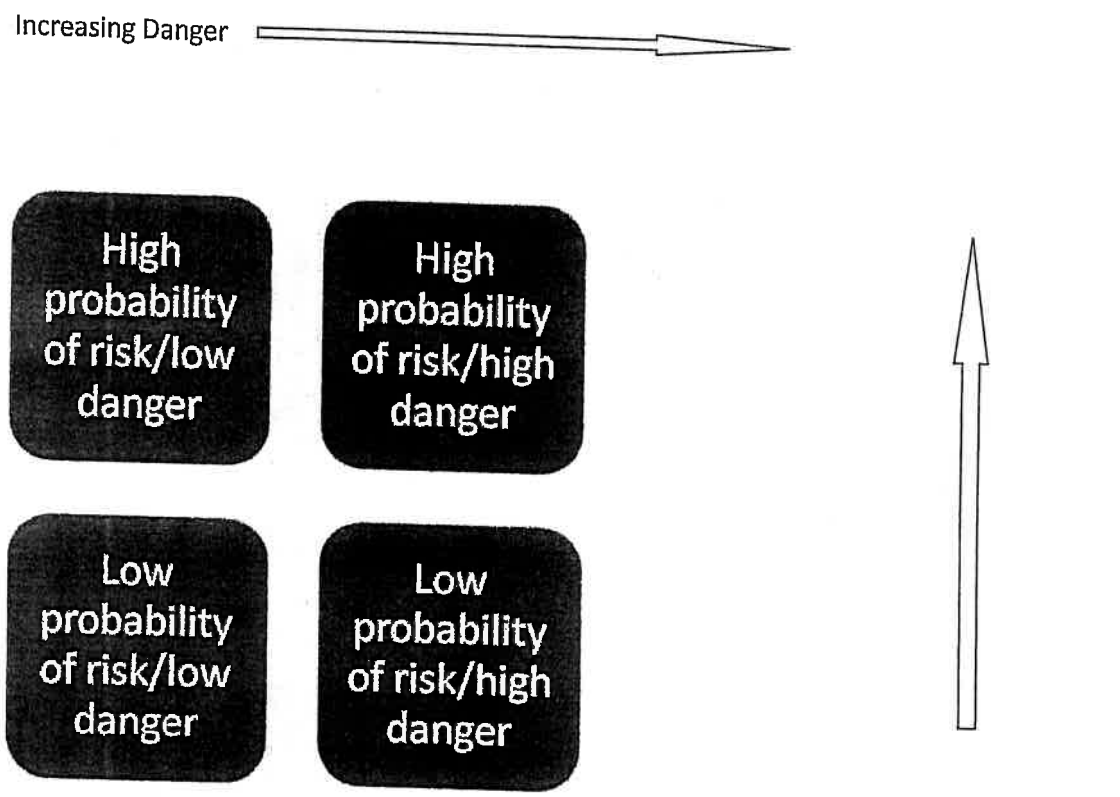
Resources:

FTC Business Guidelines, AMA Sample policy, MGMA Sample policy, Red Flag Rule Compliance Toolkit provided by Health Care Consulting Services, Inc., Identity Theft Daily, The World Privacy Forum. Resource documents available at CRPHO upon request.

Policy Created: 4/09
Policy Approved: _____
Policy Reviewed: _____

Exhibit A:

Risk Analysis Model – Use company historical experience to determine probability of risk for each item outlined in Exhibit B.



Keep in mind that not only identity theft risk is being identified, but also inappropriate access to protected health information (PHI) under HIPAA privacy and security rules.

Exhibit B - Relevant Identity Theft Red Flags Mitigation and Resolution Procedures

Identity Theft Red Flag	Prevention/Mitigation Procedure	Resolution of Red Flag*
Documents appear suspicious are provided for identification. Either forged or altered in some way.	Pause the registration process and require patient/applicant to provide additional satisfactory information to verify identity	Additional documentation must be provided to resolve discrepancy and continue registration process/patient care.
Personal identifying information provided by patient is not consistent with other personal identifying information provided by patient.	Pause the registration process and require applicant to provide additional satisfactory information to verify information	Additional documentation must be provided to resolve discrepancy and continue registration process/patient care.
If the Social Security number already exists and is associated with a different person.	Pause the registration process and require patient to provide additional satisfactory information to verify identity with the exception of patients under 18 years of age	Additional documentation must be provided to resolve discrepancy and continue registration process.
Patient has an insurance number, and cannot present a valid ID card for verification	Registration process put on hold while insurance verification takes place with carrier. Require patient to provide additional forms of identification.	Additional documentation must be provided to resolve discrepancy and continue registration process, carrier is contacted. If results of investigation do not indicate fraud, all contact and identifying information re-verified with patient.
Patient record reflects that treatment or information is inconsistent with medical history or other patterns of activity on the account	Assigned clinic staff will review previous files for potential inaccurate records. Age, race, and other physical description contradiction may be evidence of medical identity theft	If an inconsistency is identified through the review of the existing file, delay or refusal of service to patient will result. If inconsistencies are not identified, all contact and ID information is re-verified with the patient.
Patient complaints/inquiries based on receipt of: • A notice of exhaustion of benefits unexpected by patient • A bill for another patient/address discrepancy • A bill for a product or service that the patient denies receiving • A bill from a health care provider that the patient has never patronized • A notice of insurance benefits (or EOB) for health services not received • Credit report notification with inaccurate information • A collection notice on behalf of a healthcare provider never seen	Investigate complaints, follow patient complaint process. Correct all documents that are identified as clerical errors.	If inconsistencies remain following extensive review and patient complaint is still unresolved, gather all information and contact clinic designee.
Clinic is notified by law enforcement, victim of identity theft, community hospital, other clinics, or third party sources that identify theft has occurred	Investigate complaint, identify clinic risk and mark the account "invalid" to prevent possible future abuse	Suspend treatment until identity has been accurately resolved. If the results of the investigation do not indicate fraud, all contact information is re-verified with patient.

*If resolution is not found - elevate to Compliance Officer