IDENTITY THEFT DETECTION AND RESPONSE POLICY AND PROCEDURES
“Red Flags” Rule


Purpose: The purpose of this program is to assist in detecting, preventing instances of possible identity theft in connection with patients in our practice. It does so by (a) requiring us to verify the identity of all new patients, (b) establishing certain “Red Flags” that could indicate possible identity theft, and (c) requiring follow up on any incident which triggers a Red Flag. The program must be observed by all employees.

Red Flags that May Indicate Identity Theft: (these are only suggested red flags, may not include all examples).
1. An individual falsely claiming to be someone else who is known to the office staff;
2. Unexplained discrepancies between the patient’s medical records and the patient’s physical condition.
3. A report by a patient known to the office staff that he or she has been the victim of identity theft in connection with the health services provided by this agency;
4. An unrecognized individual with no personal identification or who refuses to provide information about their identity;
5. Suspicious documents that appear to have been altered or that contain information that does not match the person presenting them;
6. Altered or canceled insurance cards;
7. Attempts to submit by phone a patient’s credit card or insurance information as payment for services;
8. Any form of notice stating that a patient’s information or identity may have been stolen;
9. A notice that the patient is on active duty in the armed forces;
10. Suspicious requests for prescription or a refill;

Procedures: Any employee of this agency who encounters a probable “Red Flag” situation or any other activity that may indicate identity theft should report the situation to the Compliance Officer. That person will follow up as appropriate and will record the incident.

Employee Responsibilities, include but not limited to:
* Request identification at registration (ie: driver’s license, state ID, passport, military or school ID, etc). In the event the client does not have a photo ID, we will ask for two forms of non-photo ID, one of which has been issued by a state or federal agency (ie: Social Security card, a utility bill or company). When the client is under 18 or if the client is unable due to their condition to produce identification, the responsible party’s identification will be requested.
* Under the red flag law no one will be refused care because they do not have acceptable identification with them. Patients will be asked to bring appropriate documents to their next visit.
* If client indicates they have Medicaid, verify Medicaid status on Champs.
* Ask for Insurance card of client at each visit, make copy and place in client record.
* If client paying by credit card, be sure to look for signature on back of card. If no signature ask for photo ID. Never accept a credit card number over the phone.
* If client paying by check, be sure signed. Ask for photo id to cross reference address, check signature.
* If a red flag situation has occurred, the employee will contact the Compliance Officer/Office Manager for guidance. These individuals will determine if flagging is necessary and will make a RED check (✓) near the client’s name on their record/chart.
When Identity Theft Occurs
If a person obtains or uses (or attempts to obtain or use) the personal identifying information of another person to obtain medical services or information in the name of such other person without consent or lawful authority, our agency will take the following steps:

Notifications – When Identity theft is reasonably suspected or is known to have occurred. The client’s file will be flagged so personnel are aware that the medical record may contain inaccurate information about the client. Others to be contacted include:

a. IT Department will be contacted whenever there was a Security Breach –(ie: unauthorized access of PHI (personal health information) and 1) social security number 2) driver’s license or 3) financial account number (including credit card number.

b. The Compliance Officer will be contacted so they can report to the person whose personal information was or is reasonably believed to have been acquired by an unauthorized person. Such reporting will be made in the most expedient time possible and without delay.

c. Accounting so that all patient accounts affected by the identity theft are put on “hold harmless” pending the outcome of the investigation.

d. Report to Law Enforcement – Our Compliance Officer will provide any necessary assistance with the determining the identity of the client and provide feedback to the Registration Department, Accounting and the Security Officer of the IT Department.

- Law enforcement will be contacted.
- In order to facilitate reporting and efficient prosecution of identity theft crimes, our agency will prepare a summary of the information that we believe in good faith constitutes evidence of criminal conduct (ie: information provided by the victim and the suspect, photos, statement of value of services obtained by the suspect, etc).
- Our Compliance Officer will make reasonable efforts to limit the disclosure of protected health information of the minimum necessary to report the suspected identity theft and the information disclosed will not directly or indirectly identify what services the client received.

B. Notifying Victims of Identity theft-“When the Patient Does Not Know Identity Theft Has Occurred”
After consultation with law enforcement about the timing and content of any victim notification (to ensure notification does not impede a law enforcement investigation), victims of identity theft must be notified by our Compliance Officer. Victims of identity theft will be encouraged to cooperate with law enforcement in identifying and prosecuting the suspected identity thief.

C. Correcting Medical and Payment Records, Flagging, Verification and Releasing Bill Hold Harmless
To ensure that 1) inaccurate health information is not inadvertently relied upon in treating a client, 2) a client or third-party payer can not be billed for services the client did not receive and 3) client health information is protected from inappropriate disclosure, client medical and payment records are corrected when a case of identity theft occurs, we will do the following:

- Medical Record – After appropriate consultation with and input from the client (whose identity has been properly verified and documented, appropriate clinical personnel will make appropriate corrections to the client’s medical record to be certain the record contains correct entries only (e.g., by transferring information from the incorrect record to the appropriate record).
If the identity of the client who received the services is not known, an identity theft record will be created and the protected health information will be maintained in that record until such time as the identity of the client who received the services is known or the required record retention period ends.

A detailed explanation of the corrections will be generated by us and verified by the client. Our Compliance Officer will send amended information to persons who have received incorrect or incomplete information, if necessary. Our Compliance Officer will remove all related documents from all areas of the medical record (electronic and paper) and make replacements with appropriately revised documents. The client’s verification of the corrected medical record will be documented and included as part of the case file.

- Payment Records – after appropriate consultation with and input from the client, whose identity has been properly verified and documented, our billing department will:
  1. Make appropriate corrections to the client’s billing information.
  2. Inform and provide documentation to any third-party payer affected by the adjustments
  3. Make any necessary repayments to ensure that the client and the payer pay only for services actually provided to the client.

A detailed explanation of the corrections will be generated by us and verified by the client. The client’s verification of the corrected billing records will be documented and included as part of the case file.

- Flagging – Our Financial Manager will verify that all demographic and insurance information is correct after the visit is transferred to the appropriate record and will ensure that all related documents are removed from the billing and financial systems and replaced with appropriately revised documents. Once all medical and billing records have been corrected, the Financial Manager will release the bill hold harmless and bill appropriately.

D. Assisting Identity Theft Victims

- Copies of Records on Written Request – Identity theft victims are entitled to obtain a copy of the business transaction records, which may include billing and medical record information, maintained by our practice (or by others on our behalf) relating to the identity theft at no cost to the victim.

- We will provide these records within 30 days of receipt of the victim’s written request. Our agency also will provide these to any law enforcement agency that the victim authorizes. Note: Before providing such records, we will ask for proof of identity. We will also ask for a police report (regarding the identity theft). We will document receipt of and copy all such information.

- We may refuse to provide these records if we determine in good faith that:
  1. the true identity of the person asking for the information cannot be verified.
  2. the request for the information is based on a misrepresentation
  3. state or federal law prohibits us from disclosing such information
Clients will be referred to the State of Michigan’s web site for Identity Theft (this site has valuable information on who to contact, forms, etc) at: http://www.michigan.gov/msp/0,4643,7-123-72297_41992_72431---.00.html

E. **Recoveries from the Suspect** – If known to our agency, we will bill the identity theft suspect for unlawfully obtained services, plus consider pursuing a civil claim for restitution as part of any criminal prosecution.

F. **Accounting for Disclosures** – Our Compliance Officer will determine whether, as a result of identity theft, protected health information was inappropriately disclosed. If PHI was inappropriately disclosed, our Compliance Officer will account for such disclosures in accordance with our HIPAA policy and enter the information on a Disclosure Log in the client’s file.

G. **Update Computer Database(s)** – When identity theft is reasonably suspected, either our Financial Manager or Compliance Officer will update our Database(s) (Dentrix, MICR, Insight, etc) to include alerts on both the identity theft victim and the individual assumed responsible for the ID theft.