Systems Design EMS

Identity Theft Prevention Program

Effective beginning January 1, 2011

I. PROGRAM ADOPTION

Systems Design West ("SDW") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program was developed with oversight and approval of the compliance officer. After consideration of the size and complexity of the SDW's operations and account systems, and the nature and scope of the SDW's activities, the compliance officer and SDW's managing member determined that this Program was appropriate for SDW, and therefore adopted this Program to begin on January 1, 2011.

_____ _____

C. Mark Spice, Managing Member Date

_____ _____

Jody O'Brien, Compliance Officer Date

II. PROGRAM ASSESSMENT AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. On completion of the assessment, Systems Design West's operation is at low risk for identity theft for the following reasons:

1. Access to medical services through 911 is not currently a target for identity theft;
2. Most of our services are provided in the patient's home; and
3. In our years of experience, reports of identity stolen in order to receive ambulance services are very rare.

B. Red Flags Rule definitions used in this Program

The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as "a pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

The Rule defines creditors as any entity
(A) "that regularly and in the ordinary course of business—

(i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;

(ii) furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or

(iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person;

(B) does not include a creditor described in subparagraph (A)(iii) that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person."

"Identifying information" is defined under the Rule as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, SDW considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. SDW identifies the following red flags:

Red Flags

1. Notice from a customer, a victim of identity theft, a law enforcement agency, or someone else that an account has been opened or used fraudulently;
2. Returned mail;
3. Accounts using the same Social Security number under a different name;
4. Unauthorized database access to protected information; and
5. Patients who receive payment for ambulance services and do not apply the payment to their account.

IV. DETECTING RED FLAGS.

The following steps will be used by SDW personnel to detect the red flags listed above:

Detect

1. Be alert to phone calls or correspondence patients who have received a bill which is not theirs;
2. Be alert to phone calls or correspondence from patients who state they are a victim of identity theft;
3. Review returned mail and identify suspect accounts;

4. Notification of a breach by IT department; and
5. Unpaid accounts with record of third party payment made to the patient.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event SDW personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. When a person receives a bill and states they did not receive ambulance services, administrative personnel will research, using correct spelling of patient's name, birth date, SSN and information from other sources to determine whether there is an error, whether the patient is confused or whether there is an identity theft risk;
2. When a person receives a bill and states they are a victim of identity theft, administrative personnel will research, as in #1 above. Personnel can request an affidavit regarding their identity theft claim;
3. Returned mail is documented in account and researched using information from the hospital, Accurint and patient phone contact. If identity theft is suspected, contact Program Administrator;
4. Firewall and network security does not allow access from outside the network. All personal computers are password protected. Notify Program Administrator of any suspected or attempted breach;
5. If a patient keeps a third party payment that is due to the ambulance service, notify the compliance officer. If the patient habitually keeps payments meant for the ambulance service, the agency should be contacted so that appropriate measures can be taken. These measures can include use of a collections agency to collect on the account, face-to-face meeting with the patient or cease from billing insurance so that patient does not receive payment; and
6. Notify the Program Administrator for determination of the appropriate step(s) to take in any situation that is not covered above.

Protect customer identifying information

In order to further prevent the likelihood of Identity Theft occurring with respect to ambulance accounts, SDW will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;

2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of customer information necessary for ambulance billing purposes.

VI. PROGRAM UPDATES

The Program Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of SDW from Identity Theft. In doing so, the Program Administrator will consider SDW's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in SDW's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for SDW. The Committee is headed by a Program Administrator who is the Compliance Officer of SDW. Two or more other individuals appointed by the head of SDW or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of SDW staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

SDW staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Billing services personnel will receive annual training. IT personnel will take part in an annual review of network security.

C. Service Provider Arrangements

In the event SDW engages a service provider to perform an activity in connection with one or more accounts, SDW will take the following steps to ensure the service provider performs

its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review SDW's Program and report any Red Flags to the Program Administrator.