EXHIBIT B

SAMPLE POLICY/PROCEDURE FOR IDENTITY THEFT PREVENTION, DETECTION AND MITIGATION PROGRAM

I. Purpose and Overview.

A. The purpose of this Policy/Procedure ("Policy") is to assure that _____ ("Provider") maintains compliance with the requirements regarding the prevention, detection and mitigation of Identity Theft as set forth in the federal regulations known as the "Red Flag Rules."[1]

1. "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority. This includes "Medical Identity Theft," i.e., Identity Theft committed for the purpose of obtaining medical services, such as the use of another person's insurance card or number. Although Medical Identity Theft may occur without the knowledge of the individual whose medical identity is stolen, in some cases the use of an individual's medical identity may occur with the knowledge and complicity of that individual.

B. This Policy sets forth the steps Provider will take in implementing a program for detecting, preventing and mitigating Identity Theft (the "Program") in connection with Covered Accounts, as required by the Red Flag Rules. "Covered Account" means:

1. An account that Provider offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and

2. Any other account that Provider offers or maintains for which there is a reasonably foreseeable risk to individuals or to the safety and soundness of Provider from identity theft, including financial, operational, compliance, reputation or litigation risks.

C. Section II of this Policy describes the risk assessment Provider shall conduct at the inception of the Program and annually thereafter. Section III sets forth the "Red Flags" (i.e., warning signs) that may alert Provider personnel to the possible existence of Identity Theft in the course of Provider's day to day operations. Section IV sets forth the procedures Provider will follow in attempting to detect those Red Flags. Section V sets forth the procedures Provider will follow in responding appropriately to Red Flags that are detected, in order to prevent and mitigate Identity Theft. Section VI sets forth the procedures Provider will take in responding to a claim by an individual that he has been a victim of Identity Theft.

[1] See 16 C.F.R. § 681.2, as supplemented by the Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation set forth in Appendix A of 16 C.F.R. Part 681 ("Guidelines") and the Supplement thereto.

Section VII describes how Provider will administer the Program. Section VIII describes the annual updating of the Program.

D. Questions regarding this Policy or the Program shall be directed to the Program Compliance Officer designated pursuant to Section VII.

II. Risk Assessment

A. Upon initial implementation of the Program, and annually thereafter as a part of the annual update described in Section VIII of this Policy, Provider shall determine whether it maintains Covered Accounts. As part of that determination, Provider shall conduct a risk assessment to determine whether it offers or maintains Covered Accounts that carry a reasonably foreseeable risk of identity theft, including financial, operational, compliance, reputation or litigation risks. The risk assessment shall take into consideration:

1. The methods Provider provides to open its accounts;

2. The methods it provides to access its accounts; and

3. Its previous experiences with identity theft.

III. Identification of Red Flags

A. A "Red Flag" is a pattern, practice or specific activity that indicates the possible existence of Identity Theft. In other words, a Red Flag is a warning sign regarding the possibility of Identity Theft.

B. In identifying Red Flags relevant to its operations, Provider has:

1. Reviewed the examples of Red Flags found in the Red Flag Rules (see the Supplement to the Guidelines);

2. Considered the factors specified in Section II.A above; and

3. Incorporated Red Flags from sources such as changes in identity theft risks of which Provider becomes aware and applicable regulatory guidance.

C. Based on the process specified in the Section III.B above, Provider has identified the following situations as Red Flags that should alert Provider personnel to the possibility of Identity Theft:

1. A patient submits a driver's license, insurance card or other identifying information that appears to be altered or forged;

2. The photograph on a driver's license or other government-issued photo I.D. submitted by a patient does not resemble the patient;

3. Information on one form of identification submitted by a patient is inconsistent with information on another form of identification, or with information already in Provider's records or information obtained from other sources such as a consumer credit data base;

4. A patient has an insurance member number but no insurance card;

5. The Social Security Number ("SSN") or other identifying information furnished by a patient is the same as identifying information in Provider's records furnished by another patient;

6. The SSN furnished by a patient has not been issued, is listed on the Social Security's Administration's Death Master file, or is otherwise invalid. The following numbers are always invalid:

    a. the first 3 digits are in the 800, 900 or 000 range, or in the 700 range above 772, or are 666;

    b. the fourth and fifth digits are 00; or

    c. the last four digits are 0000;

7. The address given by a patient does not exist or is a post office box, or is the same address given by an unusually large number of other patients;

8. The phone number given by the patient is invalid or is associated with a pager or an answering service, or is the same telephone number submitted by an unusually large number of other patients;

9. The patient refuses to provide identifying information or documents;

10. Personal identifying information given by a patient is not consistent with personal identifying information in Provider's records, or with information provided by another source such as an insurance company or consumer credit database;

11. A patient's signature does not match the signature on file in Provider's records;

12. A patient contacts Provider [*or Provider's billing service*] and indicates that he or she has received an invoice, explanation of benefits or other document reflecting a transport that the patient claims was never received;

13. Mail correspondence is returned to Provider [*or Provider's billing service*] despite continued activity associated with that mailing address;

14. Provider [*or Provider's billing service*] receives a warning, alert or notification from a credit reporting agency, law enforcement or other credible source regarding a patient or a patient's insurance information;

15. Provider or a Service Provider has suffered a security breach, loss of unprotected data or unauthorized access to patient information;

16. An insurer denies coverage due to a lifetime benefit limit being reached or due to an excessive volume of services;

17. A discrepancy exists between medical or demographic information obtained by Provider from the patient and the information found in health facility records;

18. Attempts to access an account by persons who cannot provide authenticating information;

19. [R*eview list of Red Flags in the Supplement to the Guidance and add any others from that list that appear relevant*].

D. Provider shall update the foregoing list of Red Flags as part of its annual update of the Program.

E. All Provider personnel have an affirmative obligation to be vigilant for any evidence of a Red Flag and to notify their immediate supervisor, or the Program Compliance Officer, to report the Red Flag.

IV. Procedures for Identifying Red Flags

Provider personnel will follow the following procedures in order to detect the Red Flags indicated above, which indicate the possibility of Identity Theft.

A. The process of confirming a patient's identity should never delay the delivery of urgently or emergently needed medical care. When a patient's condition permits collection of demographic information and documentation, medical transport crews shall request, in addition to an insurance card, a driver's license or other form of government issued photographic personal identification. If the patient lacks such photographic identification, medical transport personnel shall:

1. Request other form of identification, such as a credit card; and/or

2. Ask a family member or other person at the scene who knows the patient to verify the patient's identity.

B. Billing personnel, in the course of creating and processing claims, and verifying patient information, shall be alert for the existence of any of the Red Flags listed in Section III above.

C. Before providing information regarding an account, or making any change to an address or other information associated with an account, the requester shall be required to provide the social security number, full name, date of birth and address of the patient. If the requester makes the request in person, a driver's license or other government issued photographic identification shall be requested.

D. In the event medical transport personnel or billing personnel encounter a Red Flag, the existence of the Red Flag shall be brought to the prompt attention of the individual's supervisor or the Program Compliance Officer so that it can be investigated and addressed, as appropriate, in accordance with the procedures set forth in Section V below.

V. Responding to Red Flags

A. When a Red Flag is detected, Provider personnel shall investigate the situation, as necessary, to determine whether there is a material risk that Identity Theft has occurred or whether there is a benign explanation for the Red Flag. The investigation shall be documented in accordance with Provider's incident reporting policy. If it appears that Identity Theft has not occurred, Provider may determine that no further action is necessary.

B. Provider's response shall be commensurate with the degree of risk posed by the Red Flag. In determining an appropriate response, Provider shall consider aggravating factors that may heighten the risk of Identity Theft, such as a data security incident that results in unauthorized access to a patient's account records, or notice that a patient has provided information related to a Provider account to someone fraudulently claiming to represent Provider or to a fraudulent website.

C. If it appears that Identity Theft has occurred, the following steps should be considered and taken, as appropriate:

1. Except in cases where there appears to be obvious complicity by the individual whose identity was used, promptly notify the victim of Identity Theft, by certified mail, using the Identity Theft Patient Notice Letter developed by Provider. Notification may also be provided by telephone, to be followed by a mailed letter;

2. Place an Identity Theft Alert on all patient care reports ("PCRs") and financial accounts that may have inaccurate information as a result of the Identity Theft;

3. Discontinue billing on the account and/or close the account;

4. Reopen the account with appropriate modifications, including a new account number;

5. If a claim has been submitted to an insurance carrier or government program ("Payor") in the name of the patient whose identity has been

stolen, notify the Payor, withdraw the claim and refund any charges previously collected from the Payor and/or the patient;

6. If the account has been referred to collection agencies or attorneys, instruct the collection agency or attorneys to cease collection activity;

7. Notify law enforcement and cooperate in any investigation by law enforcement;

8. Request that law enforcement notify any health facility to which the patient using the false identity has been transported regarding the Identity Theft;

9. If an adverse report has been made to a consumer credit reporting agency regarding a patient whose identity has been stolen, notify the agency that the account was not the responsibility of the individual;

10. Correct the medical record of any patient of Provider whose identity was stolen, with the assistance of the patient as needed;

11. If the circumstances indicate that there is no action that would prevent or mitigate the Identity Theft, no action need be taken.

VI. Investigation of Report by a Patient of Identity Theft

A. If an individual claims to have been a victim of Identity Theft (e.g., the individual claims to have received a bill for a transport he did not receive), Provider [*or its billing service*] shall investigate the claim. Authentication of the claim shall require a copy of a Police Report and either:

1. The Identity Theft affidavit developed by the FTC, including supporting documentation; or

2. An identification theft affidavit recognized under state law

B. Provider personnel shall review the foregoing documentation and any other information provided by the individual and shall make a determination as to whether the report of Identity Theft is credible.

C. The individual who filed the report shall be informed in writing of Provider's conclusion as to whether Provider finds the report credible.

D. If, following investigation, it appears that the individual has been a victim of Identity Theft, Provider will take the appropriate actions as indicated in Section V of this Policy.

E. If, following investigation, it appears the report of Identity Theft was not credible, the individual shall be notified and Provider may continue billing on the account,

upon approval of the Program Compliance Officer. The account shall not be billed without such approval.

VII. Administration of the Program

A. The Program, and all material changes thereto, shall be approved by Provider's [*board of directors/ an appropriate committee thereof/other*[2]]. (the "Oversight Body"). *[NOTE; If Provider does not have a board of directors or other governing body, the Program may be approved by an individual at the level of senior management*.]

B. A designated employee at the level of senior management shall be designated by the Oversight Body as the Program Compliance Officer and shall be responsible for the oversight, development and implementation of the Program.

C. Provider shall train staff, as needed, to effectively implement the Program. The following categories of personnel shall be trained in the implementation of the Program:

1. All medical transport personnel;

2. All billing office personnel;

3. All management personnel;

4. [*Other*].

D. Initial training shall occur no later than May 1, 2009 for all current personnel. Newly hired personnel shall be trained in the implementation of the Program as part of their standard compliance and HIPAA training. "Refresher" training shall be included in the annual compliance and HIPAA training given to Provider personnel, and may be given to specific employees from time to time on an "as needed" basis.

E. Provider shall exercise appropriate and effective oversight of all arrangements involving a service provider whose duties include opening, monitoring or processing patient accounts, or performing other activities which place them in a position to prevent, detect or mitigate Identity Theft ("Service Providers"). Each Service Provider shall be required to execute an amendment or addendum to its service agreement or business associate agreement which requires it to:

1. Implement a written Identity Theft Program that meets the requirements of the "Red Flags Rule";

[2] NOTE; If Provider does not have a board of directors or other governing body, the Program may be approved by an individual at the level of senior management.

2. Provide a copy of such Program to Provider no later than May 1, 2009;

3. Provide copies of all material changes to such Program on an annual basis; and

4. Either report all Red Flags which it encounters to Provider, or take appropriate steps to prevent or mitigate Identity Theft itself.

F. The Program Compliance Officer shall report to the Oversight Body [*or to a designated employee at the level of senior management*], on an annual basis, on compliance with the Program. The report shall address material matters related to the Program and evaluate issues such as:

1. The effectiveness of the Program in addressing the risk of Identity Theft;

2. Service Provider arrangements;

3. Significant incidents involving Identity Theft and Provider's response;

4. Recommendations for material changes to the Program.

VIII. Annual Update of the Program

The Program will be reviewed, revised and updated on an annual basis. In performing such update, Provider shall consider:

A. Provider's experiences with Identity Theft over the period since the last revision of the Program;

B. Changes in methods of Identity Theft, or in methods to detect, prevent and mitigate Identity Theft;

C. Changes in Provider's technology and operations, including any new electronic health record or financial software programs implemented by Provider; and

D. Changes in business arrangements of Provider, including but not limited to changes in its relationships with Service Providers.