American Accounts and Advisers
Identity Theft Prevention Program

Purpose

American Accounts and Advisers is committed to providing all aspects of our service and conducting our business operations in compliance with all applicable laws and regulations. This policy sets forth our commitment to compliance with those standards established by the Federal Trade Commission under the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transaction Act of 2003 ("the Red Flag Rules") at 16 C.F.R. §681.2, regarding the establishment of a written Identity Theft Prevention Program ("Program") that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

Scope

This Program contains policies and procedures designed to identify, detect and respond appropriately to "Red Flags" for identity theft. It also contains policies and procedures for the periodic identification of covered accounts and for the general administration of the Program. This Program addresses our general approach to compliance with the Red Flag Rules. As a "creditor" with "covered accounts" under the Red Flag Rules, **American Accounts and Advisers** is required to:

- Periodically identify covered accounts;
- Establish a written Identity Theft Prevention Program; and
- Administer the Identity Theft Prevention Program.

Definitions

(a) "Account" means a continuing relationship established by a person with the **American Accounts and Advisers** to obtain services for personal, family, household or business purposes and includes an extension of credit, such as the purchase or services involving a deferred payment.

(b) "Covered account" means:

(i) An account that the **American Accounts and Advisers** offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and

(ii) Any other account that the **American Accounts and Advisers** offers or maintains for which there is a reasonably foreseeable risk to individuals or to the safety and soundness of **American Accounts and Advisers** from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(c) "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority.

(d) "Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

(i) Name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number or employer or taxpayer identification number;

(ii) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(iii) Unique electronic identification number, address, or routing code; or

(iv) Telecommunication identifying information or access device (as those terms are defined in 18 U.S.C. §1029(e)).

(v) Medicare number.

(vi) Health care claim number.

(e) "Program" means this written Identity Theft Prevention Program developed and implemented by **American Accounts and Advisers**.

(f) "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(g) "Service provider" means a person who provides a service directly to the **American Accounts and Advisers** and includes third party billing companies and other organizations that perform service in connection with **American Accounts and Advisers's** covered accounts.

Procedure

1. Identify Covered Accounts

(a) **American Accounts and Advisers** will annually determine whether it offers or maintains covered accounts (see definition of "covered account" in this Program) and shall document that determination.

(b) As part of this annual identification of covered accounts, **American Accounts and Advisers** shall conduct an annual risk assessment of its accounts to determine whether it offers or maintains accounts that carry a reasonably foreseeable risk to patients or to the safety and soundness of **American Accounts and Advisers** from identity theft, including financial, operational, compliance, reputation, or litigation risks. In determining whether **American Accounts and Advisers** offers or maintains such accounts, **American Accounts and Advisers** will conduct an annual risk assessment that takes into consideration:

(i) The methods it uses to open its accounts;

(ii) The methods it uses to access its accounts; and

(iii) Its previous experiences with identity theft.

(c) The annual identification of covered accounts should ideally be conducted by an evaluation or audit team acting under the direction and control of the board or other individual in charge of Program administration.

2. Identify Red Flags

(a) Once **American Accounts and Advisers** has identified its covered accounts, it shall identify Red Flags (see definition in this Program) for those accounts. This shall be conducted on an annual basis in conjunction with **American Accounts and Advisers**'s identification of covered accounts. **American Accounts and Advisers** will also identify red flags as they arise and incorporate them into this Program.

(b) **American Accounts and Advisers** shall consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(i) The types of covered accounts it offers or maintains;

(ii) The methods it provides to open its covered accounts;

(iii) The methods it provides to access its covered accounts; and

(iv) Any incidents of identity theft that **American Accounts and Advisers** has experienced.

(c) **American Accounts and Advisers** shall also consider the examples of Red Flags listed in Supplement A to Appendix A to 16 C.F.R. Part 681. The Program shall include relevant Red Flags from the following categories, as appropriate:

(i) Alerts, notifications, or other warnings received from consumer report agencies or service providers, such as fraud detection services;

(ii) The presentation of suspicious documents;

(iii) The presentation of suspicious personal identifying information, such as a suspicious address change;

(iv) The unusual use of, or other suspicious address change;

(v) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

(d) **American Accounts and Advisers** shall also incorporate Red Flags from sources such as:

(i) New and changing risks that **American Accounts and Advisers** has identified; and

(ii) Any applicable supervisory guidance from the FTC or other appropriate sources.

(e) The following are Red Flags identified for **American Accounts and Advisers's** covered accounts as of the most recent update to this Program:

(i) Patterns of activity on payment accounts that are inconsistent with prior history;

(ii) Increases in the volume of inquiries to an account;

(iii) The presentation of information that is inconsistent with other

sources, e.g., the address, date of birth, or social security number listed for the patient does not match the address given or is inconsistent with other identifying information provided by the patient;

(iv) Personal identifying information is identified by third-party sources as having been associated with known fraudulent activity;

(v) Personal identifying information of a type commonly associated with fraudulent activity (e.g., fictitious address, use of mail drop, or phone number that is invalid or associated only with a pager or answering service);

(vi) The social security number provided by the patient is a duplicate of that of other patients;

(vii) The address or telephone numbers given are the same or similar to those of other patients, particularly recent ones;

(viii) Attempts to access an account by persons who cannot provide authenticating information;

(ix) Requests for additional authorized users on an account shortly following change of address;

(x) Uses of an account that are inconsistent with established patterns of activity such as: nonpayment when there is no history of late or missed payments;

(xi) Nonpayment of the first payment on the account;

(xii) Inactivity on an account for a reasonably lengthy period of time;

(xiii) Mail correspondence sent to the provided address is returned and mail is returned despite continued activity in the account;

(xiv) Notification of **American Accounts and Advisers** of an unauthorized transaction by the patient;

(xv) Notification of **American Accounts and Advisers** by the patient, a law enforcement authority, or other person, that it has opened a fraudulent account;

(xvi) A complaint or question from a patient based on the patient's

receipt of:

1. A bill for another individual;

2. A bill for a service that the patient denies receiving;

3. A bill from a health care provider that the patient never utilized;

4. A notice of insurance benefits (or Explanation of Benefits) for health services never received; or

5. A patient or insurance company report that coverage for legitimate healthcare service is denied because insurance benefits have been depleted or a lifetime cap has been reached.

(xvii) A complaint or question from a patient about information added to a credit report by a health care provider or insurer;

(xviii) A dispute of a bill by a patient who claims to be the victim of any type of identity theft;

(xix) A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance;

(xx) A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency;

(xxi) A security breach;

(xxii) Unauthorized access to a covered account by personnel;

(xxiii) Unauthorized downloading of patient files;

(xxiv) Loss or theft of unencrypted data;

(xxv) Inappropriate access of a covered account;

(xxvi) A computer virus or suspicious computer program;

(xxvii) Multiple failed log-in attempts on a workstation;

(xxviii) Theft of a password;

(xxix) The presentation of an insurance card or form of identification that is clearly altered; and

(xxx) Lost, stolen, or tampered facility equipment.

3. Detect Red Flags

(a) **American Accounts and Advisers** shall adopt reasonable policies and procedures to address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(i) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, and

(ii) Authenticating patients, monitoring transactions, and verifying the validity of change of address requests.

(b) The following procedures have been adopted by **American Accounts and Advisers** to address the detection of Red Flags as of the most recent update to this Program:

(i) Suspicious Documents at the Time of Transport: **American Accounts and Advisers** personnel shall be on the alert for patients who present suspicious documents such as an insurance card or form of identification that appears to have been altered or does not match other information about the patient. Whenever possible, the crew shall attempt to verify the identity of the patient with someone who knows the patient and/or someone who has rendered care to the patient. Personnel shall not delay the provision of care when verifying this information and should obtain this information after the transport when it could delay the provision of care.

(ii) ID Verification Before Discussing Patient Account Information or Change of Address: Before discussing any information related to a covered account with any individual, or making a change to address information in a covered account; **American Accounts and Advisers** personnel shall sufficiently ascertain the identity of the individual.

1. If a patient or appropriate representative makes a telephone inquiry or request regarding a patient account, **American Accounts and Advisers** personnel shall require the patient or appropriate representative of the

patient to verify the date of birth, social security number (or at least the last 4 digits), and address of the patient to whom the account pertains.

2. If the patient or appropriate representative of the patient presents in person to the business office of **American Accounts and Advisers**, s/he shall be required to provide a valid government issued photo ID in addition to the date of birth, social security number (or last 4 digits), and address of the patient to whom the account pertains.

3. If the patient or appropriate representative of the patient is unable to provide the necessary information to verify the identity of the patient, **American Accounts and Advisers** staff shall make a notation of the inquiry or address change request in the patient account file and alert an appropriate supervisor without providing access or honoring the address change request.

(iii) Under the HIPAA Privacy and Security Rules, **American Accounts and Advisers** is required to implement policies and procedures regarding the protection of protected health information and to implement administrative, physical and technical safeguards to protect electronic protected health information. The following policies and procedures from **American Accounts and Advisers**'s HIPAA compliance program serve the dual purpose of detecting identity theft in connection with the opening of and existing covered accounts at **American Accounts and Advisers** and they are hereby incorporated in this Program by reference:

(1) **General Security of Electronic and Other Patient and Business Information (Policy 1)**
(2) **Patient Access, Amendment and Restriction On the Use of PHI (Policy 4)**
(3) **Levels of Access, "Minimum Necessary Standard" and Limiting Disclosure and Use of PHI and e-PHI (Policy 10)**
(4) **Procedure for Requesting Amendment of PHI (Policy 12)**
(5) **Access to the Information System and e-PHI (Policy 16)**
(6) **Physical Security of PHI and e-PHI (Policy 19)**
(7) **Electronic Information System Activity Review and Auditing (Policy 20)**

(8) **Facility and Computer Access Point Controls (Policy 21)**
(9) **Encryption and Decryption (Policy 23)**
(10) **Use of Computer and Information Systems Equipment (Policy 25)**
(11) **Use of Electronic Mail and Facsimile Transmissions (Policy 26)**
(12) **Internet Access and Use (Policy 27)**
(13) **Computer Hardware/Peripherals/Software Inventory (Form 31)]**

4. Respond to Red Flags

(a) **American Accounts and Advisers** will respond to Red Flags of which it becomes aware in a manner commensurate with the degree of risk posed by the Red Flag. In determining an appropriate response, **American Accounts and Advisers** will consider aggravating factors that may heighten the risk of identity theft. For example, notice to **American Accounts and Advisers** that a patient has provided information to someone fraudulently claiming to represent **American Accounts and Advisers** may suggest that identity theft is more likely.

(b) **American Accounts and Advisers** shall assess whether the Red Flag detected poses a reasonably foreseeable risk of identity theft and if it does, respond appropriately. If **American Accounts and Advisers** determines that the Red Flag does not pose a reasonably foreseeable risk of identity theft, it shall have a reasonable basis choosing not to respond to the Red Flag.

(c) If any personnel at **American Accounts and Advisers** believe identity theft has occurred or may be occurring, s/he shall immediately notify a supervisor. The supervisor will contact the designated Red Flag Rule compliance officer who will determine the appropriate response.

(d) Appropriate responses may include the following:

(i) Monitoring a covered account for evidence of identity theft;

(ii) Contacting the patient;

(iii) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(iv) Reopening a covered account with a new account number;

(v) Not opening a new covered account;

(vi) Closing an existing covered account;

(vii) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(viii) Notifying law enforcement; or

(ix) Determining that no response is warranted under the particular circumstances.

(e) Patient Notification: If there is a confirmed incident of identity theft or attempted identity theft, **American Accounts and Advisers** will notify the patient after consultation with law enforcement about the timing and the content of such notification (to ensure notification does not impede a law enforcement investigation) via certified mail. Victims of identity theft will be encouraged to cooperate with law enforcement in identifying and prosecuting the suspected identity thief, and will be encouraged to complete the FTC Identity Theft Affidavit.

(f) Investigation of Suspected Identity Theft: If an individual claims to be a victim of identity theft, **American Accounts and Advisers** will investigate the claim. The following guidelines apply:

(i) The individual will be instructed to file a police report for identity theft.

(ii) The individual will be instructed to complete the ID Theft Affidavit developed by the FTC, including supporting documentation; or an ID theft affidavit recognized under state law.

(iii) The individual will be requested to cooperate with comparing his or her personal information with information in **American Accounts and Advisers's** records.

(iv) If following investigation, it appears that the individual has been a victim of identity theft, **American Accounts and Advisers** will take the following actions:

1. Cease collection on open accounts that resulted from identity theft. If the accounts had been referred to collection agencies or attorneys, the collection agencies/attorneys will be instructed to cease collection activity.

2. Cooperate with any law enforcement investigation relating to the identity theft.

3. If an insurance company, government program or other payor has made payment on the account, the provider will notify the payor and seek instructions to refund the amount paid.

4. If an adverse report had been made to a consumer reporting agency, the provider will notify the agency that the account was not the responsibility of the individual.

(v) If following investigation, it does not appear that the individual has been a victim of identity theft, **American Accounts and Advisers** or the collection agency will give written notice to the individual that he or she is responsible for payment of the bill. The notice will state the basis for determining that the person claiming to be a victim of identity theft was in fact the patient.

(g) Amendment of Records: Patient medical records and payment records must be corrected when identity theft has occurred. This is necessary to ensure that inaccurate health information is not inadvertently relied upon in treating a patient, and that a patient or a third-party payer is not billed for services the patient did not receive. Patient records will be corrected in consultation with the patient and the patient's treating health care provider(s), and in a manner consistent with the **American Accounts and Advisers's** HIPAA policy on amendments to medical records.

(h) Disclosure/Unauthorized Access to Unencrypted Data: If there is a disclosure of, or an unauthorized access to, unencrypted computerized data containing a person's first name or first initial and last name and (1) a social security number, (2) driver's license number, or (3) financial account number (including a credit or debit card number), state law governing notification of patients will be followed.

(i) The Presentation of Suspicious Documents at the Time of Transport: When a patient presents a suspicious document such as an insurance card or form of identification that is clearly altered or does not match other information about the patient, ambulance personnel shall:

1. Note the nature of the incident and circumstances surrounding the incident in an incident report or other appropriate document so that the claim is "flagged" for review.

2. If possible, attempt to obtain identifying information about the patient from other sources such as individuals who know or have treated the patient.

3. Notify the individual in charge of Red Flag Rules compliance as soon as possible after the transport about the incident and the circumstances surrounding the incident.

4. Before opening a covered account under the name given, the Red Flag Rules compliance officer, or other designated individual, shall make attempts to verify the identity of the patient though any means possible. If it appears the patient has attempted to commit identity theft, the procedures for notification and investigation of the incident (above) shall be followed.

5. Update the Program

(a) **American Accounts and Advisers** shall update this Program (including identifying Red Flags determined to be relevant) annually.

(b) The update shall reflect changes in risks of identity theft to patients or to the safety and soundness of **American Accounts and Advisers's** information. The review and update will be based on factors such as:

(i) The experiences of **American Accounts and Advisers** with identity theft;

(ii) Changes in methods of identity theft;

(iii) Changes in methods to detect, prevent, and mitigate identity theft;

(iv) Changes in the types of accounts that **American Accounts and Advisers** offers or maintains; and

(v) Changes in the business arrangements of **American Accounts and Advisers**, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

6. Administer the Program

(a) Program Oversight: The board of directors shall designate an individual who is in charge of Red Flag Rules compliance. This

individual shall be involved in the oversight, development, and implementation and administration of the Program. The individual shall be responsible for:

(i) Implementation of this Program;

(ii) Reporting to the board of directors, or an appropriate designated committee of the board at least annually on compliance by **American Accounts and Advisers** with this Program. The report shall address material matters related to the Program and evaluate issues such as:

1. The effectiveness of the policies and procedures of **American Accounts and Advisers** in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

2. Service provider arrangements;

3. Incidents involving identity theft and management's response; and

4. Recommendations for material changes to the Program.

(b) After reviewing official annual reports, the board of directors or appropriate designated committee shall approve changes to this Identity Theft Prevention Program, as necessary.

7. Train Employees

(a) **American Accounts and Advisers** will conduct a general training session for all personnel to provide them with a general overview of this Program. All new personnel shall undergo such training during their orientation process. Documentation of training, including copies of all rosters and sign in sheets showing the training dates and the names of attendees, shall be maintained for at least four years.

(b) All staff that are responsible for the administration of the Program and staff who regularly deal with covered accounts should be trained on an annual basis.

8. Oversee Service Provider Arrangements

If **American Accounts and Adviserss** engages a third party to perform an activity in connection with one or more covered accounts (*e.g.*, billing companies, collection agencies), **American Accounts and Advisers** will:

(a) Review the third party's policies for preventing, detecting, and mitigating identity theft and determine if those policies are acceptable to **American Accounts and Advisers**; or

(b) Require the third party to comply with the applicable terms of this Program through contract or agreement.

Compliance Tool 2: Sample Letter Regarding Identity Theft Incident

[American Accounts and Advisers Letterhead]

[Date]

Via Certified Mail Return Receipt Requested
[Patient Name]
[Patient Address]

Re: Suspected Identity Theft

Dear _____:

This letter addresses the unauthorized use of your name and other personal information at **American Accounts and Advisers** on [date]. [Explain factual situation and describe compromise of information in detail (*e.g.*, how it happened, information disclosed, what actions have been taken to remedy situation, etc.)]. We have reported this incident to [name law enforcement officer] at the [local law enforcement agency], who can be reached at _____. We also have placed an alert on your account in an effort to prevent further misuse of your identity.

Identity theft is very serious because it can cause severe financial harm and take a long time to correct. Medical identity theft can lead to inappropriate medical care when incorrect information is included in a patient's medical record. If you believe you are the victim of medical identity theft, you should, in addition to the measures outlined below, ask to review and make appropriate corrections to your medical record so that you receive appropriate care. For your health and safety, it is very important that your medical records do not contain information about another person. **We request your assistance in ensuring that our records about you are correct.**

We recommend that you carefully monitor explanations of benefits (EOBs) or other remittance advice or account statements received from your health insurer to determine if any other person has used your identity to obtain health care. If you receive an EOB or bill for health care services you believe you did not receive, immediately contact your insurer and the health care provider who furnished the services.

We also recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you and verify your identity before they open any new accounts or change existing accounts. Please contact one of the three major credit bureaus. Once a credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The numbers for the credit bureaus are:

Equifax:	1-800-685-1111
Experian:	1-888-397-3742
TransUnionCorp:	1-800-680-7289

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, immediately notify the credit bureaus. If you believe an unauthorized account has been opened in your name, immediately contact the financial institution that holds the account.

You should also file a police report of identity theft. [If appropriate, give contact number for law enforcement agency investigating the incident for you.] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. Creditors want the information it contains to absolve you of the fraudulent debts. You should also file a complaint with the FTC at www.ftc.gov/idtheft/ or 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

We encourage you to report any helpful information to _____ [investigating law enforcement officer] at the [local law enforcement agency]. We also encourage you to alert other area health care providers that your identifying information is being used in a fraudulent manner.

If there is anything [name of organization] can do to assist you, please call our Compliance Office (or Privacy Officer) at 800-829-5703.

Sincerely,

Michelle Scherff Sulik

Compliance Tool 3: Sample Directors' Resolution Adopting Identity Theft Prevention Program

American Accounts and Advisers
Resolution Adopting **American Accounts and Advisers** Identity Theft Prevention Program

The undersigned, being the directors of AAA, Inc., do hereby adopt, pursuant to the General Corporation Law of Wisconsin, the following resolution:

WHEREAS:

(a) **American Accounts and Advisers** finds that identity theft is a serious problem for healthcare providers in the United States;

(b) In response to the risks posed by identity theft to consumers and to the financial soundness of businesses, the United States Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

(c) The Federal Trade Commission (FTC), along with federal bank regulators, adopted regulations implementing the FACT Act (the Red Flag Rules) that require creditors to adopt a written Identity Theft Prevention Program.

(d) **American Accounts and Advisers** believes it is a creditor subject to the FTC's Red Flag Rules; and

(e) **American Accounts and Advisers** has developed a written Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft.

BE IT RESOLVED:

(1) This board of directors hereby approves the Identity Theft Prevention Program submitted.

(2)_____ **Michelle Scherff Sulik**_____is delegated responsibility for oversight, ongoing development, implementation, and administration of the program and shall have the responsibility to develop periodic updates to the program to reflect changes in risk to customers and to the safety and soundness of the organization.

Dated: ___04/29/09_____

Compliance Tool 4: Sample Language for Job Description of Red Flag Rules Compliance Officer

USER NOTE: [This language is intended to be added to an existing job description, preferably the HIPAA Privacy and/or Security Office Job Description.]

The [privacy officer or other individual] shall also be responsible for compliance with the Red Flag Rules and shall be responsible for:

(1) The implementation of **American Accounts and Advisers**'s Identity Theft Prevention Program; and

(2) Reporting to the board of directors or an appropriate designated committee of the board at least annually on compliance by **American Accounts and Advisers** with the Program. The report shall address material matters related to the Program and evaluate issues such as:

a. the effectiveness of the policies and procedures of **American Accounts and Advisers** in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

b. service provider arrangements;

c. incidents involving identity theft and management's response; and

d. recommendations for material changes to the Program.

Compliance Tool 5: Amendment to Business Associate Agreement for Red Flag Rules Compliance

USER NOTE: [This amendment may be used as an add-on to an existing Business Associate Agreement to cover Red Flag Rule Compliance. It would become a part of the original BA Agreement you had in place as a result of the HIPAA Privacy and Security Rules. You may also add this provision to any existing contract agreement that you have with a third party who performs services on behalf of your service. Of course, use of this Amendment would only be appropriate if the original BA Agreement was fully compliant with the Privacy and Security Rules.]

American Accounts and Advisers
Amendment to Business Associate Agreement

This agreement serves as an Amendment to the existing Business Associate Agreement ("BA Agreement") between **American Accounts and Advisers** ("AAA") and _____ ("Business Associate"), with an original date of _____. The parties acknowledge that acceptance of this Amendment by the Business Associate is an essential requisite to providing its contracted services to AAA.

1. This Amendment is incorporated into the existing BA Agreement between the parties and is an integral part of that agreement.

2. This Amendment shall be effective as of _____(date) as long as the existing BA Agreement has not been terminated.

3. This Amendment is executed pursuant to the requirements of the Identity Theft Red Flag Rules promulgated under the Fair and Accurate Credit Transactions Act of 2003 ("Red Flag Rules") found at 16 C.F.R Part 681.

4. The Business Associate of AAA agrees to assume the following obligations:

    a. Business Associate agrees to ensure that its activities for AAA are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

    b. Business Associate agrees to have in place policies and procedures to detect relevant Red Flags that may arise in the performance of services on behalf of AAA.

    c. Business Associate agrees that it has received a copy of AAA's Identity Theft Prevention Program and that it will take all steps necessary to comply with the policies and procedures therein.

d. Business Associate will ensure that any agent or third party who performs services on its behalf in connection with AAA's covered accounts, including a subcontractor, agrees to implement reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

e. Business Associate agrees to alert AAA of any red flag incident (as defined by the Red Flag Rules) of which it becomes aware, and the steps it has taken to mitigate any potential security compromise that may have occurred, and provide a report to AAA of any threat of identity theft as a result of the incident.

f. Business Associate authorizes termination of the BA Agreement if AAA reasonably determines that Business Associate has violated a material term of this Amendment.

Agreed to this _____ day of _____, 2009.

American Accounts and Advisers [Business Associate]

By:_____ By:_____

Its:_____ Its:_____

Date:_____ Date:_____

Compliance Tool 6: Sample Red Flag Detection/Response "Tip Sheet"

USER NOTE: [This Sample "Tip Sheet" is intended to be a "quick reference" for ambulance field personnel and billing personnel to help identify practices and situations that could be potential "red flags" for identity theft. It serves to supplement, and not replace, the "Model Identity Theft Prevention Program."]

AMERICAN ACCOUNTS AND ADVISERS

Red Flag Detection and Response "Tip Sheet"
For Prevention of Potential Identity Theft

Potential Red Flags

The following are examples of Red Flags that may occur in connection with covered accounts at **American Accounts and Advisers** but it is not an exhaustive list. Red Flags are activities that could indicate the possible existence of identity theft.

When you discover one of these potential red flags, report your observations to your supervisor and document those observations on the appropriate document (incident report, patient care report supplement, etc.)

Identify Theft "Tips" for Ambulance Field Personnel

Watch for the following:

- Information Does Not Match What Patient Tells You. At the time of transport, the patient presents identifying information that is inconsistent with other sources, e.g., the address, date of birth, or social security number listed for the patient does not match the address given to you or is inconsistent with other identifying information provided by the patient.

- Identity Documents That Look Altered. At the time of transport, if a patient presents suspicious documents such as an insurance card of form of identification that appears to be altered, you should alert your supervisor and those who receive the patient.

- Patient's Physical Description Does Not Fit What You Were Told. The patient's physical description does not meet the description of the patient during past patient transports, or is not consistent with information you received from other reliable sources, such as other crew members or hospital staff.

- Patient Name Band Inconsistent With What Patient Tells You. Check the

patient's name band in all transports from health care facilities. If the patient says he is someone other than the name on the wristband, ask the nursing staff for verification.

- Keep All Clipboards and Laptops Secure. Do not let clipboards or laptop devices out of your sight. Others may be able to obtain identity information from these things and use that information. The clipboards and laptop devices could easily be stolen if not kept in your direct custody.

- Missing Wallets, Purses, and Other Personal Effects. Report missing wallets and purses and other personal effects of those who were on the scene or in the patient's room when the loss was discovered. Notify law enforcement where appropriate.

Identity Theft "Tips" for Billing Personnel

- Others Tell You The Identity Has Been Associated With Fraudulent Activity. The presentation of personal identifying information is identified by third-party sources as having been associated with known fraudulent activity.

- Persons Accessing Accounts Cannot Provide Authenticating Information. Before discussing account information with any individual or making any changes to account information, you should obtain sufficient information from the individual to verify their identity. If the inquiry is over the phone or through other electronic means, the individual should be asked to provide the date of birth, address, and last four (4) digits of the social security number of the patient to whom the account pertains. Additionally, if the individual shows up in person, you should ask him/her to present some sort of government issued photo identification such as a driver's license. If the individual making the inquiry is not the patient to whom the account pertains, ask for verification from the person that they have permission to access the account before you grant them access to an account. If you are unsatisfied that they have authorization, you should contact the patient and notify a supervisor.

- Law Enforcement Alerts You. Law enforcement officials tell you that a specific person has opened a fraudulent account.

- You Receive Unusual Complaints About an Account. A complaint or question from a patient is received that is based on the patient's receipt of: (1) bill for another individual; (2) a bill for a service that the patient denies receiving; or (3) a notice of insurance benefits (or Explanation of Benefits) for health services never received.

- There Is A Sudden or Unexplained Loss of Electronic Data. If you

experience an unusual loss of data, you should immediately notify your supervisor and protect all devices from additional potential loss of data to the fullest extent possible.