APPENDIX A: Possible Red Flags in Connection with a Covered Account

Possible Red Flags in connection with establishment of a Covered Account may include:

1. Address discrepancies;
2. Presentation of suspicious documents;
3. Photograph or physical description on the identification that is not consistent with the appearance of the person presenting the identification;
4. Individual Identifying Information provided by a person to establish a Covered Account that is not consistent with other personal identifying information on file with System Administration;
5. Documents provided for identification that appear to have been altered or forged.

Possible Red Flags in connection with an existing account may include:

1. Any unusual or suspicious activity related to Covered Accounts
2. Notification from account holders, law enforcement, or service providers of unusual activity related to a Covered Account
3. Notification from a credit bureau of fraudulent activity regarding a Covered Account
4. A complaint or question from an Account Holder based on the Account Holder’s receipt of:
   a) a bill for another individual
   b) a bill for a product or service that the Account Holder denies receiving
   c) a bill from a health care provider that the Account Holder denies patronizing; or
   d) a notice of health plan benefits or other third party payor payments made on behalf of an Account Holder (such as an Explanation of Benefits) for health services the Account Holder never received.
5. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the Account Holder.
6. A complaint or question from an Account Holder about the receipt of a collection notice from a bill collector.
7. An Account Holder or third party payor report that coverage for legitimate hospital stays is denied because benefits have been depleted or a lifetime cap has been reached.
8. A complaint or question from an Account Holder about information added to a credit report by a health care provider or third party payor.
9. A dispute of a bill by an Account Holder who claims to be the victim of any type of Identity Theft.
10. An Account Holder who claims to have a health plan or other third party coverage or eligibility but never produces an identity card or other physical documentation of the coverage or eligibility.
11. A notice or inquiry from an insurance fraud investigator for a private insurance company or a state or federal regulatory or law enforcement agency.
12. A statement from an account holder that a bill or Explanation of Benefits was never received and the address on file is incorrect.
Possible methods of detection of Red Flags include:

1. Requiring each Account Holder to provide photo identification at each “in person” encounter, and in the case of an Account Holder seeking medical services or products, requiring a copy of the third party payor identification card at each encounter. Note: This detection method may not be appropriate for minors, indigent patients with no insurance, and emergency cases. Each department or office should determine in the risk assessment if requesting identification is unduly burdensome on their account holder population in light of the risk of Identity Theft in that population.
2. Requiring multi-factor identification before conducting any transaction relating to a Covered Account with an Account Holder over the telephone.
3. Requiring that on-line transactions come though a secure, password protected portal or in the case of a System Administration employee, a verifiable, secure password protected System Administration e-mail account.
4. Thoroughly following up on each billing inquiry from Account Holders, especially inquiries regarding care that was not received, bills for individuals not covered by the Covered Account or policies held, or bills from other health care providers that the Account Holder never visited.
5. Periodically auditing medical records to ensure that treatment is consistent for a single individual.