IDENTITY THEFT RED FLAGS INDICATORS

The following information represents examples of suspicious activity that may indicate possible identity theft. The information contained in this Attachment "A" is not all inclusive and may be updated from time to time to incorporate additional suspicious activity or information that may indicate identity theft. This information should be considered for purposes of detecting potential identity theft when verifying or authenticating a patient/student's identity or when working with a Covered Account.

1. **Credit Reporting Agency Alerts, Notifications or Warnings**. These alerts, notifications or other warnings from a Credit Reporting Agency include, but are not limited to:

   - A fraud or active duty alert included with a consumer report/credit report;
   - Notice of credit freeze in response to a request for a consumer report/credit report;
   - Notice of address discrepancy is received from the Consumer Reporting Agency;
   - A credit report shows a pattern of activity that is inconsistent with the history and usual pattern of activity of the individual (patient or student);

2. **Presentation of Suspicious Documents or Identifying Information**. This type of situation may include, but is not limited to:

   - Identification documents, such as photo identification, insurance cards, etc. appear to be forged or altered;
   - Personal identifying information (i.e., photograph, physical description) on the identification does not match the individual presenting the information;
   - Address or name does not match the information on the identification and/or insurance card(s), credit card(s), etc.
   - Other information on the identification document is not consistent with information in the file (e.g., the person's signature on a document or check does not match what is in the file); and
   - The social security number on the card has not yet been issued, is listed on the Social Security Administration's Death Master File, or is otherwise invalid. Social Security Numbers having the first 3 digits as 666 or in the 800, 900 or 000 range, or in the 700 range above 772; the fourth and fifth digits as "00" or the last four digits as "0000".

3. **Presentation of Suspicious Identifying Information.** This type of situation may include, but is not limited to:

   - The social security number is the same as one given by another individual;
   - Identifying information, such as birth date is different from other information previously provided by the individual or in the file;
   - Identifying information, such as an address, does not match information from other sources, such as credit reports, or information that is in the file;
   - Identifying information is the same as information provided by another individual or previously identified as fraudulent; and
   - An individual fails or refuses to provide identifying information (other than social security number not required by law; See HSC OP 52.08, Social Security Number Policy.

4. **Suspicious Activity.** This can include, but is not limited to:

- Mail sent to the patient/student (or a parent or legal guardian) repeatedly returned as undeliverable even though the account is still active;
- Breach in the TTUHSC EP computer system security;
- Payments stop on an otherwise consistently "up-to-date" account without any notice from the patient/student;
- Unauthorized access to or use of patient/student information;
- Notification from the patient/student that they are not receiving mail sent by TTUHSC EP;
- Change of address for an account followed by a request to change the account holder's or guarantor's name;
- Notification has been received that we have an account for a person engaged in identity theft;
- Notice from the patient/student, law enforcement or others of possible identity theft; or
- Dispute by the patient concerning the validity of a bill or the health care services/items provided, such as a claim that the health care/items listed were not received or that the patient did not receive health care services from the provider listed on the bill or explanation of benefits (EOB); and
- Receipt of any notice or inquiring into potential identity theft, including those received from an investigator, private insurance company or law enforcement agency.