## TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER

**Operating Policy and Procedure** 

HSC OP: 52.10, Identity Theft Prevention, Detection and Mitigation Program

**PURPOSE:** The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is

to safeguard the confidentiality, integrity and availability of individual identifying information, by detecting, investigating and mitigating potential identity theft in accordance with the Federal Trade Commission's (FTC) Red Flag Regulations.

**REVIEW:** This HSC OP will be reviewed every odd-numbered year (ONY) by the Institutional

Compliance Officer, the IT Security Officer, the Registrar, the Senior Managing Director

of SOM Business Office, and the Executive Director of Library Services, with recommendations for substantive revisions forwarded to the People and Operations

Council.

## **DEFINITIONS:**

For purposes of this policy, the following terms are defined as follows:

Consumer Reporting Agency is an agency, such as Experian, Equifax or TransUnion, that collects and sells information regarding the creditworthiness of a particular individual.

Consumer Report for purposes of this policy is any written, oral, or other communication of any information by a Consumer Reporting Agency bearing on an individual's credit worthiness, credit standing, credit capacity which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the individual's eligibility for credit to be used primarily for personal, family, or household purposes.1

Covered Accounts<sup>2</sup> are those accounts identified in the Red Flag Regulations<sup>3</sup> as a consumer account designed to permit multiple payments or transactions over time and any other account for which there is a reasonably foreseeable risk of identity theft. For purposes of this policy, it includes, but is not limited to, patient financial accounts,

device.5

Notice of Address Discrepancy ("Notice"). A Notice of Address Discrepancy is a notice sent

The Designated Individual shall promptly investigate any Red Flag to determine its validity. Such investigation will include, but not be limited to a review of one or more of the following:

- a. Data entry or other internal error that created the Red Flag;
- b. Existence of a filed police report of identity theft;
- c. Review of the medical record, financial records or student record, as applicable to confirm or resolve potential suspicious activity, such as signature comparison, dates of services, multiple e-raider uses from different locations, etc.;
- d. Receipt of a fraud alert listed with a Credit Reporting Agency; or
- e. Any other information to confirm or disprove identity theft.

If, after investigation, the Designated Individual believes that there is evidence of identity theft, the Designated Individual shall respond in accordance with section 7 below.

7. Investigation of Suspected Identitus.6 mm2(13/ii)2(1/5)Ta(pii)4Relic (Opir)TB)5(10/tD(53):TUTh(2005(1/54/ii)46(1/5))TUTH(2005(1/54/ii)46(1/5))TUT