



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 each year (ANN) by the Institutional Compliance Working Committee (ICWC), with recommendations for revisions forwarded to the President by May 1.

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 Accounts² are those accounts identified in the Red Flag Regulations³ 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 not limited to patient financial accounts and student financial accounts maintained by TTUHSC, or its agents.

- This policy does not apply to financial accounts related to TTUHSC employee payroll deductions which are the responsibility of Texas Tech University which processes payroll on behalf of TTUHSC.

Identity Theft is a fraud committed or attempted by an individual using another person's identifying information to obtain money, items or services, including medical care or education services to which the individual is not entitled.⁴

Identifying Information is any name or number that may be used alone or with other information to identify an individual, including, but not limited to: (1) name, social security number, date of birth, telephone/cell number, government issued driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number, protected health information (PHI), credit/debit/banking account numbers; (2) unique biometric data such as fingerprint, voice print, retina or iris image or other unique physician representation; (3) unique electronic identification number, address or routing code; IP or other computer identifying address, or telecommunication identifying information or other access device.⁵

¹ See 15 USC 1681a (d).

² See 16 CFR 681.2(b) (3).

³ See 16 CFR 681 *et seq.*

⁴ See 16 CFR 603.2 (a).

⁵ See 16 CFR 603.2 (b).

Notice of Address Discrepancy ("Notice"). A Notice of Address Discrepancy is a notice sent to TTUHSC by a Consumer Reporting Agency informing TTUHSC of a substantial difference between the address given by the individual who is the subject of the consumer report and the address(es) in the Consumer Reporting Agency's files.⁶

Red Flag is a pattern, practice or specific activity involving an individual's identifying information that indicates possible existence of identity theft to receive medical or educational services from TTUHSC.⁷

Security Breach is an incident of unauthorized access to or disclosure of data containing identifying financial, personal, and/or PHI maintained by TTUHSC where illegal use of the information has occurred or is reasonably likely to occur or that creates a material risk of harm to one or more individuals, including, but not limited to risk of identity theft.

POLICY/PROCEDURE:

1. Program Oversight and Responsibility

- a. Program Administrator. The Institutional Compliance Officer (ICO), with input from the Institutional Compliance Working Committee, shall oversee this Identity Theft Prevention, Detection and Mitigation Program, to include periodic updates to this policy reflecting changes in risks of identity theft to individuals whose Identifying Information is maintained by TTUHSC. The ICO will also provide periodic reports to the CWC on the effectiveness of the identity theft program.
- b. Designated Individual(s). Each TTUHSC School or Administrative area with Covered Accounts shall notify the ICO of those individual(s) who will have primary responsibility for identifying Red Flags related to their specific operations involving Covered Accounts and provide training to staff regarding this policy. The Designated Individuals shall continuously review and evaluate their Red Flag program effectiveness and provide an annual report to the ICO to include any recommended policy changes.

2. Vendor Contracts

Any contract between TTUHSC and a third party vendor who process any Covered Accounts for or on behalf of TTUHSC shall include language that the third party vendor agrees to comply with the FTC Red Flag Regulations.

3. Red Flags

Attachment "A" provides examples of unusual activity, suspicious documents and personal identification constituting red flags. Designated Individuals shall utilize the Red Flags identified in Attachment "A" as well as any other activity relevant to their Covered Accounts to identify possible identity theft.

4. Identity Theft Prevention and Detection

Designated Individuals are responsible for educating their staff on how to detect Red Flags (Attachment "A") that indicate possible identity theft. Schools, Campuses and Departments with Covered Accounts shall establish processes and procedures to detect Red Flags in connection with the opening of Covered Accounts and activity in existing Covered Accounts, such as the following:

- a. Patient Identity Verification. Request from a patient (or his/her parent or legal guardian) and make a duplicate copy of all current insurance cards and at least one form of valid photo identification (e.g., passport; driver's license; work photo identification card; government photo identification or any other photo identification that includes the

⁶ See 16 CFR 681.1(b).

⁷ See 16 CFR 681.2(b) (9).

individual's full name) if this information is not already in the patient's medical record. If the patient is unable or unwilling to provide this information, notify the supervisor in charge for further action.

- b. Student Identity Verification. Request information to verify the identity of a student, or his/her parent or legal guardian requesting student financial information in person, or by telephone, facsimile or e-mail. This information may include, but is not limited to, the presentation of photo identification (e.g., driver's license, passport, etc.), name, date of birth, home address, or other academic information on file with TTUHSC. If the student or his/her parent or legal guardian is unable or unwilling to provide this information, notify the immediate supervisor in charge for further action.
- c. Authentication of Patients and/or Students. At each encounter request photo identification to verify with the information in the file. If photo identification is not available, then request the individual provide an address, phone/cell number, last four of the social security number or other unique identifying information. If the information provided is incorrect or suspicious (see Attachment "A" Red Flags), then notify the immediate supervisor for further action.
- d. Requests for Changes. Verify the validity of requests to change the billing address, insurer/payer information, guarantor, or other unique identifying information.

5. **Reporting Detected Red Flags**

All TTUHSC faculty and staff have an obligation to be vigilant for any evidence of a Red Flag or other activity that might indicate a possibility of identity theft and to notify their immediate supervisor and/or Designated Individual who shall be responsible for responding in accordance with paragraphs 6 and 7 below.

6. **Investigating Reports of Identity Theft**

The Designated Individual shall promptly investigate any report of potential identity theft, whether from a student, patient or TTUHSC faculty/staff member to determine its validity. Such investigation will include, but not be limited to a review of one or more of the following:

- a. Whether the individual has filed a police report for identity theft and provided a copy of such report;
- b. Review of the medical record, financial records or student record, as applicable to determine potential suspicious activity, such as signature comparison, dates of services, etc;
- c. a fraud alert listed with a Credit Reporting Agency;
- d. Any other information to verify or disprove the claim of identity theft.

If, after investigation, the Designated Individual believes that the individual has been a victim of identity theft, the Designated Individual shall respond in accordance with paragraph 8 below.

7. **Investigation of Detected Red Flags**

- a. Patient Red Flags. The Institutional HIPAA Privacy Officer (IPO) and Institutional Information Security Officer (ISO) shall be notified of Red Flags identified related to patient Covered Accounts. The IPO and/or ISO or their designees, with assistance from the Designated Individual from the affected School or Administrative area shall promptly investigate reported Red Flags and submit a confidential written report of findings to the TTUHSC HIPAA Committee and ICO. Such reports shall be maintained by the ICO for six (6) years in accordance with HIPAA regulations.

- b. Student Red Flags. The Records Custodian for Education Records⁸ (FERPA Officer) shall promptly investigate reported Red Flags on student financial accounts and submit a confidential written report of findings to the ICO.

8. **Duty to Mitigate/Correct Identified Identity Theft**

If an investigation determines that a report of identity theft or detected Red Flags may/will result in harmful effect to a patient or student, the Institutional Compliance Officer will coordinate with the IPO, ISO and/or FERPA Officer and others as necessary to mitigate, to the extent practicable, any known harm. Such mitigation may include, but is not limited to, the following listed actions:

- Monitoring a Covered Account for evidence of identity theft;
- Opening or closing a Covered Account;
- Opening a new Covered Account with a new account number
- Changing passwords, security codes or other security devices that permit access to any TTUHSC Covered Account that contains identifying information of a particular patient or student;
- Removing inaccurate information from, and/or correcting information in the patient or student record;
- Suspend collection activity on a Covered Account;
- Notifying patient(s) or student(s) of a Red Flag event or Identity Theft in accordance with paragraph 9 of this policy; and/or
- To the extent permitted by law or contract, notifying law enforcement, payors and/or others.

9. **Notification of Actual or Suspected Identity Theft**

After the submission of a Red Flag report (paragraph 7 above), the ICO and the Office of the General Counsel shall review the report to determine whether TTUHSC has an obligation to notify the patient(s), student(s) or other individuals affected by any actual or potential security breach. If it is determined that a security breach has occurred and notice is required, the affected individuals shall be notified by appropriate means, as determined by the ICO and the Office of General Counsel, to include, but not limited to, providing the type of identifying information involved, information about how to alert Credit Reporting Agencies and a TTUHSC contact for further information and assistance. Any delay in notification due to a request from law enforcement shall be documented, including the name of the law enforcement individual making the request and the law enforcement agency. TTUHSC shall comply with the notice requirements under Texas Business and Commerce Code, Section 48-103, as applicable.

10. **Notice of Address Discrepancy Received From Consumer Reporting Agency**

Upon TTUHSC's receipt of a Notice of Address Discrepancy ("Notice"), the following actions **shall** be taken:

- a. Confirm Identity. Determine that the individual for whom the consumer report was requested is the same as the individual identified in the Notice, which may include the following:
 - Compare the information in the consumer report with the information TTUHSC has in its files regarding that individual;

⁸ See HSC OP 77.13, Student Education Records under the Family Educational Rights and Privacy Act (or FERPA)

- Verify the information in the consumer report with the individual who is the subject of the consumer report.
- b. Confirm Address. If the individual's identity is confirmed to be the same as the individual who is the subject of the consumer report, confirm the accuracy of the individual's address, which may include the following:
- Verify the address with the individual who is the subject of the consumer report;
 - Review TTUHSC records to verify the address is correct; or
 - Review third party materials, such as leases, utility bills, etc. to verify the address is correct.
- c. If the individual's identity is confirmed and the address is verified, notify the entity that sent the Notice of the individual's correct address.
- d. If the individual's identity or address cannot be confirmed or verified, contact the Institutional Compliance Officer.

11. **Right to Change Policy**

TTUHSC reserves the right to change, modify, amend or rescind this policy in whole or in part at any time without the consent of its employees.