



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 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 is not limited to, patient financial accounts, student financial accounts, library patron accounts, or other covered accounts maintained by TTUHSC or its agents.

- This policy does not apply to financial accounts related to TTUHSC employee payroll deductions that 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 without authority 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 identification number (i.e., e-raider), 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 physical representation; (3) unique electronic identification number, address or routing code; IP or other computer identifying address, or telecommunication identifying information or other access

¹ See 15 USC 1681a (d).

² See 16 CFR 681.1(b) (3).

³ See 16 CFR 681 *et seq.*

⁴ See 16 CFR 603.2 (a).

device.⁵

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 and Risk Committee (ICRC), 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 ICRC 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 and report any security breaches to the ICO.

2. Vendor Contracts

Any contract between TTUHSC and a third-party vendor who processes 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 suspicious personal identification constituting Red Flags. Use the information contained in Attachment "A" to identify possible identity theft.

4. Identity Theft Prevention and Detection

The ICO shall periodically provide educational resources to Designated Individuals on the FTC Red Flag Rules and this policy.

Designated Individuals are responsible to educate 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

⁵ See 16 CFR 603.2 (b).

⁶ See 16 CFR 641.1(b) and 16 CFR 681.2, Appendix A, Supplement A.

⁷ See 16 CFR 681.1(b) (9).

following:

- a. Patient Identity Verification. Request that a patient (or his/her parent or legal guardian) provide, and make a duplicate copy of all current insurance cards, and, where available, at least one government issued photo identification (ID) card (e.g., passport; driver's license; school ID card; military ID, or government ID) if this information is not already in the patient's medical record. In the case of minor children who do not have a government issued photo identification card, use the parent or legal guardian's photo identification. If the patient is unable or continually refuses to provide this information, notify the supervisor in charge for further action. The supervisor may seek further guidance from the ICO. Departments may use the GE Red Flag module to establish patient identity verification processes in place of, or in addition to, obtaining a patient's government issued photo ID.
- b. Student Identity Verification.
 1. Student Business Services Office. 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 ID (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. The student must grant authority for information on their account to be released to another individual, including a parent.
 2. Office of Financial Aid. Student identity is verified through the Department of Education (DOE) from which TTUHSC downloads information. Any discrepancies identified by the DOE are forwarded to the TTUHSC Office of Financial Aid which processes the notifications in accordance with federal and state laws.
 3. Registrar's Office: Request that student identity is verified primarily through photo identification (TTUHSC ID, driver's license, passport, etc.). If photo identification is not available, the student will be requested to provide a number of personal identifying information details including, but not limited to, social security number, address, phone number, email address, date of birth or other academic information on file with TTUHSC. If the information provided is inaccurate or suspicious, the Registrar will be notified immediately for further action.
- c. Reports of Suspicious Activity. 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, social security number, insurer/payer information, guarantor, or other unique identifying information. Verification can include checking the proposed new information against an official document, such as a government issued ID for change of a social security number, payer insurance card for change of insurance/payer information, or current utility bill for change of address.

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 Sections 6 and 7 below.

6. **Investigating Reports of Identified Red Flags**

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 Identity Theft/Reports

- a. Patient Covered Accounts. The HIPAA Privacy Officer (PO) and Institutional Information Security Officer (ISO) shall be notified of instances of potential identity theft related to patient Covered Accounts. The PO and/or ISO or their designees, with assistance from the Designated Individual from the affected School or Administrative area shall promptly investigate and submit a 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 Covered Accounts. The Records Custodian for Education Records⁸ (Registrar) shall promptly investigate instances of potential identity theft on student financial accounts and submit a confidential written report of findings to the ICO.
- c. Red Flags – Library Patrons. The Director of Library Services shall promptly investigate instances of potential identity theft to library patron accounts and submit a confidential written report of findings to the ICO.

8. Duty to Mitigate/Correct Identified Identity Theft

If an investigation in section 7 determines that identity theft occurred that may/will result in harmful effect to a patient or student or other individual, the ICO will coordinate with the RPO, ISO and/or the Registrar 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;

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

- Notifying the potential victim of identity theft in accordance with Section 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 (section 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 identity theft. If it is determined that identity theft 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 date, name of the law enforcement individual making the request and the law enforcement agency. TTUHSC shall comply with applicable notice requirements under Texas Business and Commerce Code, Chapter 521, Unauthorized Use of Identifying Information, and as it may be amended.

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

Any Department/School requesting a consumer report from a Consumer Reporting Agency that receives a Notice of Address Discrepancy ("Notice"), **shall** take the following actions:

- 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;
 - 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 ICO.

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, students or patients.