TRS Policy Confidentiality

Purpose

To protect the confidentiality of information, by properly identifying and protecting it from unauthorized disclosure, access, or public release as required by law, legal agreement, or by TRS policies and procedures. And to notify employees and third parties, including non-TRS workers, of their responsibility to properly classify and secure TRS information.

Core Values

This policy ties to the TRS Member Focused, Accountability, and Ethics Core Values as it is everyone's responsibility to protect TRS information and report any unauthorized access or use of this information.

References

TAC 202.24:(b): State agencies are responsible for: (1) defining all information classification categories except the Confidential Information category, which is defined in Subchapter A of this chapter, (Confidential Information is "information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement") and establishing the controls for each.

Texas Government Code Sec. 2054.161, Data Classification, Security, and Retention Requirements. On initiation of an information resources technology project, including an application development project and any information resources projects described in this subchapter, a state agency shall classify the data produced from or used in the project and determine appropriate data security and applicable retention requirements under Section 441.185 for each classification.

Texas Government Code, Chapter 552 (Public Information Act)

Texas Government Code Sec.411.083

Applies To

All TRS employees, TRICOT employees, and non-TRS workers

Note: TRS agents, independent contractors, non-TRS workers assigned to TRS, and other third parties must adhere to this policy while on TRS premises or working remotely, while conducting TRS business, or while otherwise holding, collecting, assembling, maintaining, or having access to TRS information.

Definitions

Classification: Arrangement of information into categories according to a set of established criteria.

Confidential Information: information that is identified as such by federal or state law, TRS policies and

procedures, as well as information typically excepted from public disclosure through specified statutory carve outs or through decisions by the Open Records division of the Texas Office of the Attorney General. Access to this information should be very limited.

Examples of "Confidential Information" include protected health information (PHI), participant records and information about those records, information relating to the Human Immunodeficiency Virus (HIV) infection or related illness of an individual, personally identifiable information (PII), pre-investment and post-investment diligence information, and criminal history record information,

Some information classified as Confidential is information that TRS is prohibited from releasing and its disclosure is subject to criminal penalties.

Contract Sponsor: The chief officer or the person with delegated authority to initiate the purchasing and contracting process for the business area requesting the goods or services.

Criminal History Record Information: Criminal record history information obtained from the Department of Public Safety (DPS), Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division, or another law enforcement agency. Specific use of this information is related to TRS employees or applicants for employment; or non-TRS workers (contract workers, unpaid interns, and volunteers).

Critical Information: Information determined to be essential to TRS' mission and functions, the loss of which would have a significant negative impact.

HIPAA: The Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

Individually Identifiable Health Information (IIHI): information including demographic data, that relates to:

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, social security number.)

See Protected Health Information definition below.

Information Asset: Information that has value to the organization, regardless of its physical form or characteristics.

Information Owner: A person with statutory or operational authority for specified information (e.g.,

supporting a specific business function) and responsibility for establishing the controls for its generation, collection, processing, access, dissemination, and disposal.

Information Resources: The information maintained by or for TRS and the procedures, equipment, software, and data that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

Participant: A TRS member, former member, retiree, annuitant, beneficiary, alternate payee, participating in one or more of TRS benefit programs (including a health-benefit program enrollee), or person eligible for one or more of TRS benefit programs.

Personally Identifiable Information (PII): Information that can be used to individually identify a person. PII includes: individual first name or first initial and last name in combination, with one or more of data elements, such as: social security number, date and place of birth, mother's maiden name, driver's license number, state identification card number, passport number, financial account number, or other unique identifying number, characteristic, or code. PII also includes information that TRS determines could be used to identify an individual, including data derived from records of individual TRS participants.

Protected Health Information (PHI): Individually identifiable health information (IIHI) that is received, transmitted, or maintained by TRS in any form or medium. The Privacy Rule does not protect individually identifiable health information that is held or maintained by entities other than covered entities or business associates that create, use, or receive such information on behalf of the covered entity. TRS is a covered entity, as such all IIHI that the TRS health plans receives, transmits, or maintains is PHI.

Public Information: Information subject to the Public Information Act (Texas Government Code, Chapter 552). "Public information" includes information made, transmitted, maintained, or received by TRS or a TRS officer or employee in connection with TRS' official business. It also includes information produced or maintained for TRS by a third party in connection with TRS business if TRS owns the information, has a right of access to it, or pays for its production or maintenance.

Records of Individual TRS Participants or Information About the Records of Individual Participants (Participant Record Information): Records of individual TRS participants that are in the custody of the system or in the custody of an administering firm, a carrier, or another governmental agency, including the comptroller, acting in cooperation with or on behalf of TRS or information about such a record.

Security Incident: An event resulting in accidental or deliberate unauthorized access, loss, disclosure, modification, or destruction of information resources.

Sensitive Information: Information that although subject to public release under a PIA request should afforded a higher level of protection and be vetted and verified before its release to ensure Confidential data (e.g., net salary information, PHI) is not comingled.

Third Party: An entity or individual, including a TRS contractor, which conducts business on behalf of or in

cooperation with TRS or provides goods or services to TRS.

Unauthorized Disclosure or Access: Includes unauthorized disclosure, release, access, transfer, dissemination, modification, misuse, destruction, or otherwise communicating all or part of any confidential information orally, in writing, or by electronic or any other means to a person or entity, or using confidential information in a manner that is *not*:

- authorized by law, rule, legal agreement, or TRS policy and procedures or
- authorized in writing by an individual or entity with authority to give permission for the release of or access to the confidential information.

Policy Statement

Each TRS information asset, regardless of its form, is classified, managed, and protected based on its contents.

When classifying information assets, TRS complies with all applicable laws, rules, and regulations that provide guidance on how to protect the confidentiality of information and TRS does not disclose information classified as Confidential to unauthorized parties.

In addition to complying with applicable data classification and protection laws, rules, and regulations, TRS establishes its own policies and procedures to protect information TRS has designated as Confidential but that is not specifically made confidential by law, rule, or regulation.

Employees, TRICOT employees, and non-TRS workers:

- Are required to read the *Confidentiality Policy, Information Security Policies and Standards, Confidential Information Procedures and Standards,* and applicable departmental/divisional Data Protection Policy and Procedures and understand the requirements to classify information assets and secure Confidential information.
- Are required to only request and be given authorized access to Confidential information only when access is necessary to perform their assigned duties or to conduct TRS business.
- Are required to protect Confidential information from unauthorized disclosure and not disclose or provide access to Confidential information except as permitted by law, regulation, or rule, or TRS policies and procedures.
- Are required to only disclose the minimum amount of information necessary to accomplish the purpose of the disclosure.
- Are required to read and adhere to TRS' HIPPA Privacy Policies and HIPAA Security Policies.

TRS will ensure that TRS agents, non-TRS workers, independent contractors, vendors, and other third parties have notice of any applicable confidentiality requirements and, before access is granted to them, understand their responsibility to protect confidential information from unauthorized disclosure as required by law. rule, regulation, or TRS policies and procedures and agree to the same.

Confidential Information:
A) Background Checks

TRS is authorized to obtain criminal history record information from DPS and the FBI, CJIS department, to manage and reduce exposure to risk, including fraud or theft, and to maintain a safe workplace by ensuring that all persons with access to TRS facilities and information resources are subject to an appropriate employment eligibility verification and criminal background check (CBC).

Criminal history record information may not be released or disclosed to any person except:

- on court order; or
- with the consent of the person who is the subject of the criminal history record information; or
- to a federal agency as required by federal law or executive order.

Criminal history record information obtained is destroyed after the information is used for the specific purposes outlined by Texas Government Code 411.083.

B) Remote Work

The same standards for maintaining confidentiality that apply to employees working at their on-site TRS office apply equally when working remotely. Employees working from remote workspaces are expected to maintain the confidentiality of TRS and trust participant information as required by law or TRS policies and procedures.

Employees working remotely may need to take additional steps to ensure protection of confidential information based on their location. For example, when working remotely employees:

- must not print off TRS information.
- must not leave their computer unlocked if there are others with access to the house.
- must not allow others, even family members to use their TRS issued computer.
- must use a privacy screen when working where others are present.
- must discuss other precautions to take with their manager.

For persons authorized to obtain criminal history record information, it is not approved to be accessed when remote working.

C) Classifying Information

Information assets are classified Confidential, Sensitive, or Public. Information classified "Confidential" for TRS business purposes may not be specifically confidential by law, rule, or regulation. Confidential information requires a higher level of protection than information classified as Sensitive or Public.

On a biennial basis, information owners recertify information classified as high risk by reviewing and updating their departmental/divisional Data Protection Policy & Procedures document, including the corresponding data protection worksheet.

D) Disclosures

TRS complies with the procedures and disclosure requirements of the Texas Public Information Act with regard to information designated as confidential for TRS business purposes.

In accordance with TRS policies and procedures and, as appropriate, in consultation with a department Chief or a director, and Legal & Compliance, information owners may exercise discretion in releasing Sensitive or Public information pursuant to a permissive law.

TRS cannot sell PHI by state law and maintains the "non-sale" circumstances described in the TRS HIPAA Privacy Policies.

E) Monitoring Responsibility

Directors or department Chiefs will designate information owners for their information resources. The information owners are responsible for identifying and classifying information, approving, or establishing access requirements, assigning custody, and specifying and working with Information Security to identify and communicate security controls for information assets. Managers will provide guidance to TRS employees and non-TRS workers for adherence to this policy. Information owners and Information Security Office are responsible for monitoring compliance with classifying and protecting confidential information.

F) Reporting Noncompliance & Security Incidents

All employees must immediately report noncompliance with this *Confidentiality Policy* to their designated information owners or manager, the Privacy Officer, or Chief Compliance Officer. Non-TRS workers must report noncompliance with this policy to their contract sponsor.

If an unauthorized disclosure of or unauthorized access to systems containing Confidential information is suspected, immediately contact the following:

A) If an unauthorized disclosure or access of Protected Health Information, contact the Privacy Officer.

B) If an unauthorized disclosure or access of criminal history record information is suspected, or employee

confidential information immediately contact the Chief Organizational Excellence Officer, the Deputy Chief of Organizational Excellence, and the Director, L&C Business Administration

C) If an unauthorized disclosure of or unauthorized access to systems containing TRS contracts immediately contact the Director of Procurement & Contracts, and the Director, L&C Governance & Procurement Solutions.

D) If an unauthorized disclosure of or unauthorized access to systems containing TRS member PII immediately contact the Chief Benefit Officer and the L&C Director, Pension.

In addition, the Chief Information Security Officer and IS must be contacted in the event of all breaches. TRS investigates all allegations of unauthorized disclosure or access and does not retaliate against anyone who in good faith reports noncompliance with this policy or reports a security incident.

G) Training

Confidentiality and HIPAA training is provided to new employees within 30 days of employment and annually thereafter. Departmental/divisional specialized HIPAA training is provided annually, and documentation of completion is maintained by Operational Excellence.

Contract sponsors will ensure non-TRS workers are identified to receive TRS Confidentiality and HIPAA training according to the *Non-TRS-Worker Intake and Exit Procedures*.

Information related to the protection of confidential information is routinely communicated and readily available to TRS agents, employees, and non-TRS workers.

Violations

An employee who makes an unauthorized disclosure of Confidential information is subject to corrective action, which may include termination without warning, as provided in the TRS *Corrective Action Policy*.

An agent, non-TRS worker, independent contractor, vendor, or other third party who makes an unauthorized disclosure of Confidential information is subject to any sanction or penalty available by contract or law.

If required by law, certain illegal activities will be reported to the proper law enforcement agencies.

Cross Reference/Related Documents

- Remote Work Policy
- TRS Background check policy
- Information Security Policies and Standards
- TRS HIPAA Privacy Policy

- TRS HIPAA Security Policy
- TRS Corrective Action Policy
- Non-TRS Worker Intake and Exit Procedures
- Non-TRS Worker Policy

Policy Type: Agency	**First Issued:** August 2017
Contact: Privacy Officer	**Last Review: November** 2024
Department Sponsor(s): L&C	**Next Review Due Date:** November 2029
Reviewing Department(s)/ CO-Sponsors: Organizational Excellence Information Security Office	**Version Number**: V.3 2025
Review Cycle: 5 years	**Version Approved Date:** 2/11/2025
Intranet Location: L&C SharePoint Policy Page	DocuSigned by: Caasi Lamb 5E9E8D6ECA374E3...

This policy does not constitute a contract, a promise or guarantee of employment, or a guarantee of access to TRS premises or information resources, as applicable, and may be modified, superseded, or eliminated by TRS without notice to the employee.