Confidentiality

Purpose

- To protect the confidentiality of information from unauthorized disclosure or access as required by law or by TRS policies and procedures.
- To notify employees and third parties, including non-TRS workers, of their responsibility to classify and secure TRS information.

Applies To

All TRS employees

Note: TRS agents, independent contractors, non-TRS workers assigned to TRS, and other third parties are required to 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: For purposes of this policy and related procedures, information maintained by or for TRS that must or may be withheld from public disclosure under a law, either a constitutional provision, statute or judicial decision.

> Examples of "confidential information" under this policy and related procedures may include protected health information (PHI), a participant record and information about that record, information relating to the Human Immunodeficiency Virus (HIV) infection or related illness of an individual, personally identifiable information (PII), participant record information, pre-investment and post-investment diligence information, sensitive information, vital or critical information, criminal history record information, and nonpublic information.
>
> Legally, information that is "confidential by law" is information that TRS is prohibited from releasing and its disclosure is subject to criminal penalties. Other law may permit TRS to withhold certain information at TRS' discretion but does not make disclosure subject to criminal penalties. In accordance with TRS policies and procedures and, as appropriate, in consultation with the Executive Council or a director, information owners may exercise discretion in releasing information pursuant to a permissive law. But in implementing this policy and related procedures, TRS employees and contractors must handle information subject to permissive release as if it were confidential. In addition, this policy and related procedures treat the other information categories covered by them as "confidential" to facilitate compliance with the policy and implementation of the procedures by information owners, employees, and contractors.

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), FederalBureau 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.

> Examples of HIPAA information may include protected health information (PHI), personally identifiable information (PII), and individually identifiable health information (IIHI).

Individually Identifiable Health Information (IIHI): Health information that is created or received by a health care provider, health plan, or health care clearinghouse and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual, or with respect to which there is reasonable basis to believe the information can be used to identify the individual.

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, program participant (including a health-benefit program enrollee), or person eligible for TRS benefits.

Personally Identifiable Information (PII): Information that can be used to individually identify a person. Conventional PII includes the following: first name or first initial and last name in combination with one or more of the following data elements, but not limited to, 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 other than the conventional personal identifiers listed above 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 transmitted or maintained by TRS in any form or medium.

Public Information: Information subject to the Public Information Act (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 maintained by TRS that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness.

Third Party: An entity or individual, including a contractor, that 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, TRS rule, 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.

Vital Information: Information that is necessary to resume or continue TRS' business, recreate its legal and financial status, or preserve the rights of TRS, its employees, and its participants.

General Statement

Each TRS information asset is classified, managed, and protected based on its confidentiality.

TRS complies with all laws, rules, and regulations that protect the confidentiality of information maintained by TRS and does not disclose confidential information to unauthorized parties. Additionally, TRS establishes policies and procedures to protect information designated as confidential for TRS business purposes but not specifically made confidential by law, rule, or regulation. 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.

Employees and non-TRS workers:

- Are required to read the *Confidentiality Policy, Information Security Policy and Manual, Confidential Information Procedures and Standards,* and departmental/divisional Data Protection Policy and Procedures and are knowledgeable of the requirements to classify and secure TRS confidential information.
- Are 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 do not disclose or provide access to confidential information except as permitted by law or TRS policies and procedures.
- Only disclose the minimum amount of information necessary to accomplish the purpose of the disclosure.

TRS ensures that 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, they agree to protect confidential information from unauthorized disclosure as required by law or TRS policies and procedures.

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;
- 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.

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.

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

Classifying Information

Information assets are classified as high risk, medium risk, or low risk as defined in the *Information Security Manual,* Section 6.3 (Classifying TRS Information). Information classified as high risk is designated "confidential" for TRS business purposes but may not be specifically confidential by law, rule, or regulation. High risk information requires a higher level of protection than information classified as medium or low risk. Information designated by TRS as "confidential" includes the following information categories: confidential by law, HIPAA, sensitive, and vital or critical information.

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.

Monitoring Responsibility

Directors or Executive Council members designate 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 communicating security controls for information assets as defined in the *Information Security Manual*, Section 6.0 (Security Planning and Administration). Managers provide guidance to division and department employees and non-TRS workers for adherence to this policy.

Information owners and the Information Security Officer are responsible for monitoring compliance with classifying and protecting confidential information.

Reporting Noncompliance & Security Incidents

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

If an unauthorized disclosure or access of HIPAA or confidential information is suspected, immediately contact the following:

- Privacy Officer in Legal & Compliance (HIPAA information)
- Information Security Officer (Confidential information—non-HIPAA)

If an unauthorized disclosure or access of criminal history record information is suspected, immediately contact the following:

- Chief Human Resources Officer
- Assistant Director of Human Resources
- Information Security Officer (Confidential information—non-HIPAA)

TRS investigates all allegations of unauthorized disclosure or access and does not retaliate against anyone who reports noncompliance with this policy or reports a security incident. Refer to the

Information Security Manual, Section 4.0 (Reporting Information Resources Security Incidents) for further guidance.

Training

Confidentiality and HIPAA training is provided to new employees within 30 days of employment and biennially thereafter for current employees. Departmental/divisional specialized HIPAA training is provided annually and documentation of completion is maintained by Human Resources.

Contract sponsors will ensure non-TRS workers are provided individual training on confidentiality and HIPAA 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.

Corrective Action

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 *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.

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.