TEACHER RETIREMENT SYSTEM OF TEXAS

HIPAA SECURITY POLICIES & PROCEDURES

Effective: November 1, 2019

Introduction

HIPAA is the responsibility of everyone at the Teacher Retirement System of Texas (TRS) who uses, discloses or maintains Protected Health Information (PHI). This document provides the Security Policies and Procedures for compliance with 45 C.F.R. Parts 160, 162, and 164 ("HIPAA Regulations") for the secure management of PHI. These Security Policies and Procedures should be read in conjunction with the TRS HIPAA Privacy Policies and Procedures.

TRS administers three trust funds for the benefit of active and retired public school teachers in the State of Texas: (a) the Pension Trust Fund; (b) the TRS-ActiveCare Trust Fund; and (c) the TRS-Care Trust Fund. The Pension Trust Fund provides retirement benefits and death benefits to eligible retirees, including benefits based on a member's disability. Disability determinations require the use of PHI. TRS-ActiveCare provides medical and prescription drug benefits to eligible active public school employees and their eligible dependents; these employees must be employed by participating entities in TRS-ActiveCare. TRS-Care provides medical and prescription drug benefits to eligible retirees and their eligible dependents; these retirees have been employed by public school districts and charter schools in the State of Texas during their teaching careers. Each of these programs and their respective trust funds will be referred to in these Policies and Procedures as a "Plan" and collectively they will be referred to as the "Plans."

TRS will be referred to as the Plan Sponsor in these Security Policies and Procedures. The vast majority of PHI associated with the operations of TRS-Care and TRS-ActiveCare is handled by the Third-Party Administrators and Pharmacy Benefit Managers of the Plans.

The Plan Sponsor and the Plans designate themselves as a single Covered Entity for purposes of HIPAA Regulations compliance. Due to the integrated nature of providing benefits under the Plans to TRS members, active employees, and retirees, TRS made the determination to treat all Health Information maintained by all three Plans as PHI under the HIPAA Regulations. As a result, these Security Policies and Procedures apply to the PHI held by all three Plans. These Policies and Procedures do not apply to information that is not Health Information or PHI. The TRS Information Security Manual (ISM) provides guidance for the privacy and security of information that is not PHI. Except where necessary to provide integrated service to TRS members, active employees, and retirees, or where otherwise provided in these Security Policies and Procedures, PHI associated with one of the Plans should be used solely in connection with that Plan. The vast majority of PHI associated with the operations of TRS-Care and TRS-ActiveCare is handled by the Third-Party Administrators and Pharmacy Benefit manage of these two Plans.

Due to the integrated nature of providing benefits under the Plans to TRS members, active employees, and retirees, TRS made the determination to treat all Health Care maintained by all three Plans as PHI under the Privacy Regulations and the Security Regulations. As a result, these Policies and Procedures apply to all three Plans and the PHI held by the three Plans. Except where necessary to provide integrated service to TRS members, active employees, and retirees, or where otherwise provided in these

Policies and Procedures, PHI associated with one of the Plans should be used solely in connection with that Plan.

Terms used, but not otherwise defined, in these Policies and Procedures have the meanings set forth in the Glossary located at the end of this document, the Privacy Policies and Procedures, and in the HIPAA Regulations. TRS reserves the right to change these policies and procedures at any time.

Contacting the Plans' Information Security Officer: The Information Security Officer of TRS (the "Information Security Officer") is Frank Williams. He may be contacted at (512) 542-6787, or via the Information Security ("IT Security") department at ITSecurity@trs.texas.gov. Questions on these Policies and Procedures may also be directed to the Chief Compliance Officer, Heather Traeger. She may be contacted at (512) 542-6884.

Policy & Procedure for Security Management Procedures

Purpose

To outline the procedures for secure management of electronic Protected Health Information (ePHI), including risk analysis and management, and security management, evaluation and maintenance.

Applicability

This policy is applicable to all TRS divisions and offices that create, receive, maintain or transmit ePHI, including employees and Non-TRS workers (as described in the Non-TRS Workers policy).

References

Reference: 45 C.F.R. § 164.308(a)(1)(i) & (ii)(A) & (B)

Reference: 45 C.F.R. § 164.308(a)(8)

Reference: 45 C.F.R. § 164.306(e)

Policy

Anyone at TRS who accesses, uses, discloses or maintains ePHI is responsible to practice security management in compliance with HIPAA. This includes all employees and non-TRS workers. The Information Security Officer is responsible for overall periodic risk analyses, compliance program evaluations (in coordination with the Chief Compliance Officer), and maintenance.

Procedures

1. Risk Analysis
    (a) The Information Security Officer will assist TRS divisions and offices who maintain ePHI to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. The analysis should attempt to identify all relevant losses that could occur if security measures are not in place. Department-level risk analyses must be conducted at least every two (2) years or as needed based on significant environmental or operational changes to the unit security of ePHI. Examples of such changes include: significant security incidents, significant changes to the organizational or technical infrastructure, hardware and software upgrades, and changes to information security requirements or responsibilities that impact ePHI.
    (b) The Information Security Officer is responsible for conducting a TRS-wide risk analysis and for retaining documentation of the risk analysis. The Information Security Officer will conduct a TRS-wide risk analysis as needed in response to significant environmental or operational changes to the TRS-wide security environment, but under no circumstances, no less than every two (2) years. At a minimum, risk analysis documentation should identify the potential risks and vulnerabilities to the confidentiality, integrity or availability of ePHI.

(c) All Business Associate Agreements (BAAs) and Data Use Agreement (DUAs) must include a Data Management and Security Plan approved by the Information Security Officer, prior to submitting for signature.

2. Risk Management

(a) The nature of TRS necessitates that divisions and offices who create, receive, maintain or transmit ePHI must implement reasonable and appropriate security measures sufficient to reduce risks and vulnerabilities to ePHI confidentiality, integrity, and availability. The risk management decisions must be based on the required risk analysis above. Risks can be accepted, transferred, mitigated or avoided. TRS divisions and offices who create, receive, maintain or transmit ePHI may follow the risk management graph below in determining what actions to take with identified risks:

High Value of Data x Low Risk = Mitigate

High Value of Data x High Risk = Avoid or Mitigate

Low Value of Data x Low Risk = Accept

Low Value of Data x High Risk = Accept

(b) TRS divisions and offices who work with ePHI must create a risk management plan that addresses all reasonably anticipated threats or hazards to the security of ePHI. The Information Security Officer must approve the submitted plan. After approval, divisions and offices must implement and follow their risk management plans and provide the Information Security Officer with documentation of all adopted decision-making practices, implementation of analysis findings, and policies and procedures. ePHI must be protected against any reasonably anticipated inappropriate uses or disclosures pursuant to the TRS HIPAA Privacy Policies. The Information Security Officer shall work in conjunction with the Chief Compliance Officer and the Information Technology (IT) Department to create a risk management plan at an enterprise level. It is the responsibility of anyone at TRS who creates, receives, maintains, or transmits ePHI to practice security management. All violations of this policy are subject to the TRS Corrective Actions Policy.

3. Maintenance

Division and office security measures must be reviewed and modified by such divisions and offices and the Information Security Officer as needed to continue provision of reasonable and appropriate protection of ePHI. These measures must be reviewed on at least an annual basis. All unit reviews and any modifications of security measures must be documented and then retained by the Information Security Officer.

4. Evaluation

(a) All security policies and procedures adopted by TRS at either an entity-wide or division or office-level must be periodically evaluated to assure continued viability in light of technological, environmental, or operational changes that could affect the security of ePHI. Divisions or offices with ePHI are responsible for evaluating their

policies and procedures and upgrading their policies and procedures if needed, in response to significant environmental or operational changes to their environment, but under no circumstances no less than every two (2) years. All evaluations and changes to policies and procedures must be documented and sent to the Information Security Officer.

(b) Working with the individual TRS divisions and offices, the Information Security Officer shall perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the Security Regulations and subsequently, in response to environmental or operational changes affecting the security of ePHI. This evaluation must establish the extent to which TRS Security Policies and Procedures meet the requirements of the Security Regulations. This evaluation must be performed no less than every two (2) years and in response to significant environmental or operational changes to the security of ePHI at a campus-level. This evaluation must be documented along with any changes to policies and procedures resulting from the evaluation.

(c) In coordination with the Chief Compliance Officer, the Information Security Officer must immediately perform an evaluation if changes are made to the HIPAA Security or Privacy Regulations or new federal or State laws are implemented that affect the privacy or security of ePHI.

5. Documentation Retention

All documentation pursuant to this policy must be kept for a period of at least six (6) years from the date of creation of the document or the date when the document was last in effect, whichever is later. Documentation pursuant to this policy (including risk analysis documentation) must be stored securely.

Policy & Procedure for Security Incidents and Breach Notification

Purpose

To define a security incident involving ePHI and provide the procedures for notification, investigation, and reporting both during and after a security incident.

Applicability

This policy applies to all electronic data maintained by any employee or non-TRS worker. Any data used for administrative, research, or Health Care purposes is subject to this policy.

References

45 C.F.R. § 164.308(a)(6)

§ 2054.1125(b), Texas Government Code

Policy Statement

All TRS employees and non-TRS workers have the responsibility to report any real or suspected security incident to the proper TRS authority immediately. It is the responsibility of the individual to whom the suspected security incident is reported to follow the procedures outlined in this policy.

Procedures

1. Security Incident

An ePHI security incident is an attempted or successful acquisition, unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

2. Response and Reporting

TRS is required to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of known incidents; and document incidents and their outcomes. This includes improper network activity and misuse of outside data as referenced in the ISM – 3.0 "Acceptable Use of Information Resources".

3. Suspected Incident Occurs

Access may occur through a misuse of IT resources that results in a widespread intentional or unintentional compromise of information security. Large-scale intrusions into a computing network may lead to unauthorized access to sensitive information. A lost or stolen laptop may result in a security incident involving sensitive data.

4. Incident Detected

Incidents may be detected through many different means with varying levels of detail. Automated detection capabilities include network-based and host-based intrusion detection systems, antivirus

software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected; others are almost impossible to detect without automation. If the incident is a life threatening activity or an activity on a critical system, it must be reported immediately upon discovery. If the activity includes access to non-critical systems or unauthorized activity, it must be reported within two (2) hours of discovery.

5. Do Not Disturb

The incident may require further investigation. It is important that nothing be disturbed at this step of the procedure.

6. Report

Telephone 512-542-6318 or email ITSecurity@trs.texas.gov to report the incident.

7. Categorize Incident

The Information Security staff who receives the report must categorize the incident as:

(a) Denial of Service — an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing departments (CPU), memory, bandwidth, and/or disk space.

(b) Malicious Code — refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or integrity of the victim's data. Malicious code is usually designed to perform these inappropriate functions without the user's knowledge. Viruses, worms, and Trojan horses are considered forms of malicious code.

(c) Unauthorized access— occurs when a person gains logical or physical access without permission to a network, system, application, data, or other resource. Unauthorized access is typically gained through the exploitation of operating system or application vulnerabilities, by getting hold of usernames and passwords, or social engineering.

(d) Inappropriate Usage — occurs when a legitimate user violates acceptable computing use policies. Examples of inappropriate use include sending spam promoting a personal business, sending email perceived as harassing individuals, etc. Inappropriate use issues may not constitute a security incident, but must be assessed by the Information Security Officer to determine if the inappropriate usage has created a security incident.

(e) Multiple Component — a single incident that encompasses two or more incidents or falls into multiple incident categories. These incidents should be handled in line with the severest infraction involved.

8. Investigation and Initial Determinations

(a) Level 1 Investigation

(i) As soon as reasonably possible after the incident is reported, the Information Security Officer will work with IT and the impacted department or office to conduct an initial investigation of the incident. Once this initial investigation

has been conducted, which shall take place no later than the following business day after the incident is detected, the Information Security Officer will contact the Privacy Officer of TRS (the "Privacy Officer") and the TRS Chief Compliance Officer.

(ii) If this initial investigation has determined the facts of the incident, then within fifteen (15) business days after the incident is detected, the Information Security Officer and the Privacy Officer will make an initial determination as to (i) whether any ePHI, or for that matter, whether any non-ePHI, is involved in the incident and then (ii) whether any ePHI, or for that matter, if any non-ePHI, involved in the incident was Unsecured or Secured. A final determination on these issues will be undertaken in coordination with the Chief Compliance Officer as described elsewhere in these policies and procedures and in the HIPAA Privacy Policy and Procedure for Securing PHI and Addressing Breaches.

(b) Level 2 Investigation

(i) If the facts of the incident cannot be determined during the initial investigation of the incident, the Information Security Officer will call an ad hoc meeting of appropriate individuals to comprise an incident response team (the "Response Team") to investigate the incident. The Response Team shall include the Privacy Officer and may include any of the following members or their representatives, as determined by the Information Security Officer and the Privacy Officer to appropriately investigate the incident:

A. Members of the Executive Council
B. Management of affected department or office
C. Public Relations
D. Police (TRS)
E. Appropriate IT personnel
F. Enterprise Risk Management
G. Others

(ii) This expanded investigation must be conducted no later than ten (10) business days after the incident is detected. Once the Response Team has determined the facts of the incident, the Information Security Officer and the Privacy Officer will make an initial determination within fifteen (15) business days after the incident as to whether (i) any ePHI, or for that matter, whether any non-ePHI, is involved in the incident and then (ii) whether any ePHI, or for that matter, if any non-ePHI, involved in the incident was Unsecured or secured. A final determination on these issues will be undertaken in coordination with the Chief

Compliance Officer as described elsewhere in these policies and procedures and in the HIPAA Privacy Policy and Procedure for Securing PHI and Addressing Breaches.

9. Determination, Notification and Documentation Regarding Breaches and Risk Assessments.

(a) If it is determined that no acquisition, access, use or disclosure in fact exists, or that the acquisition, access, use or disclosure involves no PHI, or that the acquired, accessed, used or disclosed PHI was secured, then no breach has occurred. The Privacy Officer, in coordination with the Information Security Officer, will reduce this determination to writing in a disclosure report (the "Preliminary Disclosure Report") within 30 business days after the incident is detected.

(b) If the initial determination concludes there was an unauthorized acquisition, access, use, or disclosure of unsecured ePHI, then the Privacy Officer will follow the policies and procedure as set forth in the HIPAA Privacy Policy and Procedure for Securing PHI and Addressing Breaches, to perform the required risk assessments and breach determinations, notifications, and documentations. Accordingly, after the initial determination, all ePHI breach, assessment, notification and documentation activities will be managed by the Privacy Officer in coordination with the Information Security Officer, Chief Compliance Officer, and with the assistance and cooperation of involved TRS departments and offices, as appropriate.

(c) In either instance, the Information Security Officer will document the security incident consistent with the TRS Information Security Manual, including the investigation of the facts of the incident, and will report the incident to the Texas Department of Information Resources consistent with § 2054.1125(b), Texas Government Code. The Information Security Officer is responsible for retaining documentation of incidents.

10. Conclusion

The Information Security Officer, IT and/or the Response Team, in coordination with the Chief Compliance Officer, should determine if policies or procedures need to be implemented to prevent a re-occurrence of the incident or if additional enterprise-wide education or purchase of network or computing security devices are needed to prevent similar future incidents.

Policy & Procedure for Auditing

Purpose

To require that computer systems containing ePHI possess technical mechanisms and administrative processes that protect the confidentiality, integrity, and availability of the software and data they maintain.

Applicability

This policy covers the hardware, software and/or procedural mechanisms implemented by TRS units to record and examine activity in information systems that contain or use ePHI. Computers covered by this policy include desktop systems, laptops, handheld devices, database servers, application servers, data management systems, and infrastructure devices.

References

45 C.F.R. § 164.308(a)(1)(ii)(D)

45 C.F.R. § 164.308(a)(5)(ii)(C)

45 C.F.R. § 164.312(b)

Policy Statement

TRS shall assess potential risks and vulnerabilities by reviewing information system activity, and developing, implementing, and maintaining appropriate administrative, physical, and technical security measures in order to detect and minimize security violations involving ePHI. These protective measures give TRS the ability to identify unauthorized data access activities, assess security safeguards, and respond to potential weaknesses.

Procedures

1. General

   TRS maintains a comprehensive internal security control program, which is coordinated by the Information Security Department. Procedures, policies and record keeping activities have been established to ensure proper legal, ethical and business practices via the Information Security Manual (ISM) and other related policies. This program complements the user authentication process and may act as a deterrent to internal abuse by making users aware that audit trails, file access reports, and security incident tracking reports are produced, reviewed and investigated. Violations are subject to applicable sanctions. The internal security control program may take various forms including regular information system activity review. These reviews incorporate login monitoring, automated reports of audit trails or logs, file access reports, and manually produced security incident tracking reports.

2. Audit Controls

IT Security will centrally monitor audit records from firewall and other network protection layer logs, domain logs including login and data access activity, and event logs from mission critical server operating systems.

3. Audit Control and Review Plan

An Audit Control and Review Plan must be developed by each division or office that hosts ePHI and must be approved by the Information Security Officer. If the division or office's ePHI inventory changes, causing its Audit Control and Review Plan to change, the Plan must be re-evaluated and re-submitted to the Information Security Officer. The plan must include:

(a) Systems and applications to be logged
(b) Information to be logged for each system
(c) Login reports for each system

Procedures to review all audit logs and activity reports, including employee or non-TRS worker responsible for performing the audit, the frequency the audit is to be performed, and escalation procedures if suspicious activity is detected.

4. Audit Trail

The audit trail provides a means to monitor user activity and detect suspicious activity and/or breaches. It also provides the ability to reconstruct events where data integrity may be questioned and functions as a deterrent to misuse by employees and non-TRS workers. The audit trail process includes the implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

5. Audit Trail Mechanisms

The mechanisms used to capture audit trail information may include use of automated tools designed to report suspicious activity or use of automated warning messages that appear prior to access of sensitive information. Each division or office with systems containing medium and/or high risk ePHI (determined during the regular risk assessment) must log activity. The system hardware, software, and applications must have the capability of creating log files. These logs must include, but are not limited to:

(a) User ID
(b) login date/time
(c) activity time

Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity. Audit control mechanisms for systems containing low risk ePHI (determined during the regular risk assessment) are not required.

6. Employee and Non-TRS Worker Accountability

Divisions and offices must educate their staff on their specific audit procedures and requirements as necessary. This includes incorporating the concept of audit trail and individual user accountability.

7. Information System Activity Review

Department or offices that host ePHI must regularly have records of information system activity, such as audit logs, file access reports, and security incident reports reviewed by the Information Security department. Routine review of information systems activity provides an automatic trail of user actions whenever ePHI is accessed or modified. This review promotes individual user accountability and gives TRS the ability to reconstruct significant events or examine suspicious activities as necessary.

8. Conducting the Review

The Information Security Officer must designate the individuals responsible for conducting the review of information systems activity and determine the frequency with which the review will be conducted, based on the unit's Audit Control and Review Plan. To support an effective review, the following information should be examined: audit trails or logs; file access reports; and, security incident tracking reports. If suspicious activity is detected, the reviewer should collect: type of event; date and time of occurrence; User ID; and, program used.

9. Misuse

If misuse or suspicious activity is discovered, the division or office head and Information Security Officer must be contacted.

10. Login Monitoring

As part of the unit Audit Control and Review Plan, TRS must monitor login success and failure to systems that host ePHI. To ensure that unauthorized login attempts are discovered, discrepancies or unusual login patterns must be reported to the department or office head and Information Security Officer. Monitoring of audit trails should be performed with the help of an automated alerting tool or periodic manual review of the logs. Departments or offices must educate members of their staff on their specific procedures and reporting requirements for log-in monitoring.

11. Retention

Audit trails, file access reports, and automated security incident reports in exact and retrievable copy form must be retained in a secure manner, taking into consideration system capability, space issues, and modality. The method of retention and length of time these reports are to be retained is to be determined at the unit level and included in the Audit Control and Review Plan. All unit procedures, documentation of decisions made, information system activity reviews, and investigations conducted pursuant to this policy must be retained for a period of no less than six (6) years from the date the policy was last in effect or from the date the decision or investigation was made.

Policy & Procedure for Employee and Non-TRS Worker Security

Purpose

To outline procedures to ensure that TRS employees and non-TRS workers have appropriate access to ePHI and to prevent those who should not have access from obtaining access. This policy includes information access management, workstation use and security, and access control mechanisms.

Applicability

This policy applies to control access of ePHI at TRS by TRS employees and non-TRS workers. This includes access authorization, modification and termination procedures, use of and security of workstations containing ePHI, and access control mechanisms.

References

45 C.F.R. § 164.308(a)(3)(i) and (ii)

45 C.F.R. § 164.308(a)(4)(i) and (ii)(B) – (C)

45 C.F.R. § 164.308(a)(5)(ii)(B)

45 C.F.R. § 164.310(b) and (c)

45 C.F.R. § 164.312(a)(1)

45 C.F.R. § 164.312(a)(2)(i) and (iii)

Policy Statement

All TRS employees and non-TRS workers are responsible for managing and protecting the information technology resources under their purview. Employees are also responsible for enforcing policies regarding the administration of IT resources in their areas. The TRS IT department offers central disk storage and backup services which departments and offices use for maintaining their data. While IT systems meet the HIPAA physical security and contingency planning requirements, departments must still take care to address controls for workstation security, account management, and controlling to ePHI they create or store. It is the responsibility of all TRS employees and non-TRS workers who Access ePHI from any device and in any capacity at TRS to follow this policy.

Procedures

1. Access to ePHI

   The use and access of TRS's information systems is restricted to appropriately identified, validated and authorized individuals. TRS healthcare business operations are the only approved reasons for accessing ePHI. All other access may only occur pursuant to permission to access ePHI. Permission includes valid HIPAA authorization from an individual, Data Use Agreement (DUA), business associate agreement (BAA), or decedent research certification. Each division or office that maintains

or provides access to ePHI is responsible for ensuring that any necessary employee and non-TRS worker clearance procedures have been followed before authorizing access to ePHI. Employees and non-TRS workers shall only be granted access to the minimum necessary ePHI that they require to perform their duties. To set up access to an IT-managed resource, an account request form must be completed. This process provides the ability to document access granted, modified, or terminated. The completion of this access establishment, modification or termination will be communicated to the requestor via e-mail. Separate authorization requests are required for temporary employees, remote access, and any other special access of TRS systems. Department and office managers / supervisors must re-evaluate access rights when an employee or non-TRS worker's access requirements to ePHI change. Department and office managers / supervisors or other approved individuals are responsible for submitting the appropriate form to TRS IT when an employee or non-TRS worker's access requirements have changed. TRS IT will maintain an audit trail of requests for creation, modification, or termination of access to ePHI.

2. Termination of Access:

(a) It is the responsibility of the division or office manager/ supervisor, his/her designee, or sponsor of a non-TRS worker to submit the appropriate form to TRS IT when an employee or non-TRS worker's employment or affiliation with TRS is terminated or his or her access needs have ended.

(b) In coordination with TRS Organizational Excellence, TRS IT will disable user accounts if it finds that there has been a separation of employment or termination of assignment, even if the appropriate forms have not been submitted.

(c) TRS IT maintains the right to disable user access when it finds a breach that endangers the security of ePHI.

3. Workstation Use and Security

Each employee and non-TRS worker must use a unique user name and strong password to access ePHI. Computer workstations accessing ePHI must maintain security configurations that restrict access to ePHI to only those individuals that have been legitimately granted access. Recommended security configurations include, but are not limited to:

(a) enabling a password protected screen saver

(b) setting computers or applications to automatically terminate a computing session after a set period of idle time

(c) the use of TRS standard anti-virus products

(d) applying security patches to computer software applications and operating systems

TRS employees and non-TRS workers must adhere to the TRS Information Security Manual which outlines expectations regarding the ethical and permissible use of TRS computing resources. The TRS Confidential Information Procedures & Standards also address the proper identification, protection and disposal of confidential information. Use of shared user accounts to access ePHI must be granted in advance by IT for special purposes only. Employees and non-TRS workers inappropriately sharing user names and passwords may be subject to revocation of accounts or other

sanctions. TRS IT will disconnect workstations from the network that pose a threat to TRS information systems due to a suspected policy violation, workstation intrusions, virus infestations, and other conditions which might jeopardize TRS information or work. TRS IT will periodically scan workstations and servers for vulnerable software. TRS employee and non-TRS workers must follow the provisions of the TRS IT Security Information Security Manual in regard to guarding against, detecting, and reporting malicious software. TRS employees and non-TRS workers shall not attempt to alter audit records or avoid accounting for computing services (see TRS Information Security Manual). TRS employees and non-TRS workers shall not use TRS resources to develop or execute programs that could infiltrate the systems or alter the software components of the workstations. Workstations storing ePHI or that may be used to access ePHI must be located in areas with controlled access. An electronic audit trail of access must be maintained. It is the responsibility of the managers of that department to establish user. All suspected policy violations, workstation intrusions, virus infestations and other conditions which might jeopardize TRS information systems, data, or business must be immediately reported to the Information Security Officer.

4. Documentation

All documentation required by this policy must be retained for a period of six (6) years from when it was created or was last in effect, whichever is later.

Policy & Procedure for Facility and Device Security

Purpose

To outline the procedures for granting, modifying, and terminating physical access to electronic information systems and the facilities in which they are housed. TRS has adopted this policy to ensure that physical access to ePHI is appropriately limited.

Applicability

This policy applies to all department or offices in any physical site that houses information systems that contain ePHI. All employees and non-TRS workers who have access to ePHI and physical sites housing ePHI must also follow this policy.

References

45 C.F.R. § 164.310(a)

45 C.F.R. § 164.530(c)

Policy Statement

It is the responsibility of Security Operations, Facility Management, Organizational Excellence, and all affected department and office managers and supervisors to limit physical access to their electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is not delayed.

Procedures

5. Facility Access Controls

TRS maintains ePHI in various forms throughout its facilities. Facility access controls protect the devices or locations that hold ePHI using a variety of methods, while ensuring that properly authorized access is allowed.

6. Facility Security Plan

Security Operations maintains Building Access Control Procedures and Restricted Access Procedures to safeguard the facility, systems, and the equipment used to store or access ePHI against unauthorized physical access, tampering, and theft. These procedures should be reviewed and updated by Security Operations as needed.

7. Access Control

(a) Physical Security Operations controls access to each TRS facility pursuant to its Physical Security Policy and will permit physical access to areas that house ePHI only as directed, in writing, by the area owner. Security Operations periodically requires that each area owner review the list of people granted access to that area to determine whether a business need for access still exists.

(b) The area owner must limit physical access to areas where ePHI is maintained or can be accessed to only those employees and non-TRS workers whose role or function necessitates the use of ePHI, and should take into account at what time(s) access will occur and under what conditions. When Security Operations has received written authorization from the area owner to grant access to a particular person, Security Operations will add that access to the person's access badge, which includes the person's picture. All TRS employees and non-TRS workers are required to wear their badges while on TRS property.

(c) If an employee or non-TRS worker's access needs change or end, the department manager should immediately notify Security Operations, in writing, to modify or terminate the individual's access. Security Operations & Facility Management are responsible for maintaining a record of all employees and non-TRS workers who are granted physical access to areas that house ePHI, or information systems with ePHI.

8. Visitor and Contractor Access

(a) Visitors and contractors must be accompanied or escorted by a TRS employee or non-TRS worker who has authorized access to an area where ePHI is stored or may be accessed.

(b) Visitor and contractor access may be subject to authorizations, business associate agreements (BAAs), confidentiality agreements, etc.

9. Maintenance Records

Security Operations & Facility Management must retain records documenting physical repairs and modifications to facilities housing ePHI. Documentation may include repairs and modifications to the physical components of a facility such as hardware, walls, doors and locks, and other such components. Physical Security Operations is responsible for maintaining records on all installations, repairs, or replacements of access control devices at TRS locations.

10. Contingency Operations

In situations when TRS is seeking to restore lost data under its disaster recovery plan(s), access to critical information systems' sites will be governed by the Plan(s) and emergency access controls, as outlined in the Contingency Planning policy.

11. Control Mechanisms

Physical Security Operations & Facility Management will adopt appropriate physical control mechanism to safeguard ePHI or systems used to access ePHI. Security Operations & Facility Management may control physical access to these areas by implementing various controls, such as:

(a) Electronic security systems or physical intrusion detection systems

(b) Monitoring systems

(c) Visitor policies

(d) Alarms and various other locking systems
(e) Physical keys, swipe cards, keypads, and biometric devices
(f) Placement of security guards
(g) Name badges and badge readers
(h) Equipment enclosures, equipment identification, and fasteners
(i) Physical building construction reinforcements for secure areas (including wall, ceiling, and door materials)
(j) Proper lighting of secure areas
(k) Fire prevention, detection and suppression

12. Documentation and Records Retention

All documentation required by this policy must be retained for a period of six (6) years from when it was created or was last in effect, whichever is later.

Policy & Procedure for Transmission Security

Purpose

To implement reasonable and appropriate technical security measures for all ePHI in transit, to guard against unauthorized access to and improper alteration or destruction of the ePHI.

Applicability

This policy applies to ePHI that is transmitted over an electronic communications network (local area network, Internet connection, wireless, dial-up lines, high speed access, sending files, e-mail or facsimiles originating from computer based software applications). It is the responsibility of anyone who transmits or makes available for disclosure ePHI in any capacity at TRS to follow this policy.

References

45 C.F.R. § 164.312(a)(2)(iv)

45 C.F.R. § 164.312(e)

Policy Statement

The TRS IT Department shall put in place and shall maintain appropriate enterprise and network perimeter controls that will ensure the automatic protection of ePHI in transit.

Procedures

1. Transmission Security

Transmission security refers to the secure exchange and preservation of data over electronic communications networks. Divisions or offices that will transmit ePHI over an electronic communications network must first weigh the risk of unauthorized access to or modification of the ePHI during transmission. The division or office must then work with the Information Security department to implement a reasonable and appropriate transmission security measure to adequately address the risk to the ePHI. When transmitting ePHI electronically, regardless of the transmission security measure being used, departments and offices must take reasonable precautions to ensure that the receiving party is who they claim to be, has a legitimate need for the ePHI requested, and is being sent only the minimum necessary ePHI when the purpose of the transmission is not for Treatment, Payment, or Health Care operations. If ePHI must be transmitted over an electronic communications network and no transmission security is available please see the "Exceptions to Secure Transmission" section below. TRS web sites containing ePHI that will be accessed from the Internet must be accessed via secure file transfer or remote login protocols. ePHI transmitted via facsimile (fax) using computer-based programs to send or receive the ePHI shall comply with all technical transmission security measures.

2. Transmission Security Measures

If ePHI is being transmitted over an electronic communications network, a reasonable and appropriate transmission security measure must be implemented to adequately address the risk to the ePHI.

3. Encryption and Decryption

(a) All transmissions of ePHI from TRS to a recipient outside the TRS network (e.g., over the Internet) must utilize an encryption mechanism between TRS and the receiving entity or the file, document, or folder containing the ePHI must be encrypted before transmission.

(b) Files containing ePHI to be transferred across the Internet must be transferred using a secure medium, such as a secure file transfer protocol.

(c) E-Mail messages containing ePHI intended to be transmitted outside the TRS network must be encrypted and transmitted using the approved secure messaging product in use by TRS. See the Secure E-Mail Transmission policy below.

4. Other Methods

As other transmission security measures are investigated and approved by IT they will be added as options here. If a department or office would like to use a security method other than encryption it must first receive written approval from the Information Security Officer.

5. Integrity Controls

Departments sending ePHI over an electronic communications network must work with the Information Security department to implement transmission security measures to ensure that ePHI is not improperly modified during transmission. ePHI integrity shall be sustained using approved mechanisms (e.g., checksums, hashing algorithms, electronic signatures and digital signatures) whenever available and feasible to protect against unauthorized alteration, tampering, corruption, or falsification of the ePHI.

6. Exceptions to Secure Transmission

Situations may arise when it is infeasible to comply with the above secure transmission controls. If this occurs, care should be taken that all possible methods have been investigated. Permission for insecure transmission must be received in writing from the Information Security Officer prior to the transmission. After receiving permission for insecure transmission, departments and offices sending ePHI insecurely must make certain to minimize the ePHI sent and to redact any highly sensitive information if possible.

Policy & Procedure for Contingency Planning

Purpose

To help meet TRS's goal of protecting the availability, integrity, and confidentiality of ePHI, TRS has developed policies and procedures for responding to an emergency or other unexpected negative event or occurrence that may damage any system containing ePHI.

Applicability

This policy applies to every department and office within TRS that administers computer systems containing ePHI.

References

45 C.F.R. § 164.308(a)(4)(ii)(B)

45 C.F.R. § 164.308(a)(7)

45 C.F.R. § 164.310(d)(2)(iv)

45 C.F.R. § 164.312(a)(2)(ii)

Policy Statement

TRS shall ensure that ePHI is protected and accessible after an event occurs that prevents normal business operations and access procedures. It is the responsibility of departments and offices that house ePHI to do the same at a department or office-level.

Procedures

1. Contingency Planning

In order to assure that ePHI is available and secure during an emergency, each mission critical department and office within TRS that administers systems containing ePHI shall maintain a comprehensive plan for responding to emergencies. This plan shall describe contingency mode operations as well as steps to be taken to ensure the ability to carry on business functions if there is a disaster. ePHI held at TRS by the IT department is protected by and subject to the TRS' contingency plan which is created and maintained by the Strategic Initiatives department.

2. Contingency Plan

Specifically, each mission critical department and office contingency plan should describe mechanisms to:

(a) Avoid interruptions to critical functions even while undergoing or recovering from a loss of electricity, fire, system failure, vandalism, natural disaster, or other occurrence where systems and data are threatened;

(b) Minimize impact on total business operations by minimizing interruptions to critical functions so that they occur only infrequently, are brief in duration, and do not result in loss of business functionality; and,

(c) Address complications and consequences of normal lost processing time, operations degradation, lost equipment replacement processes, insurance funds, alternative processing sites, temporary office space, equipment, key personnel, telephones, and other business basic equipment.

3. Components of Contingency Plan

In coordination with the Risk Management department, the department or office manager, working with other key administration personnel, must create, obtain management approval, implement, maintain, and periodically review a contingency plan which includes the following components:

4. Data Backup and Storage Plan

The Data Backup and Storage Plan must provide for the creation and maintenance of an exact retrievable copy of ePHI in the department. Backups should also be made prior to movement of equipment hosting ePHI. The plan may include maintenance and retrieval of paper files of Protected Health Information (PHI).

5. Backup

TRS requires that an exact retrievable copy of the organization's ePHI is created. Backups are to be created in the most appropriate form and in a timely manner. Note that the frequency and methodology of the back-up is directly dependent on the importance of the data to the organization, system complexity, system configuration, resources and value of data. Regardless of the frequency or methodology, backup data should be created and rotated often enough to avoid disruption if current files are lost or damaged.

6. Scheduling, Labeling, and Off-Site Storage

One copy of ePHI (daily, weekly, or monthly version) must be labeled and maintained on the department's premises in a secure manner. An additional copy of ePHI (daily, weekly or monthly version), or a duplicate of the backup, must be maintained off-site in a manner that is environmentally secure and limited by physical access controls to prevent improper modification and to limit access to appropriate users only. The off-site location should be geographically different from the department's location so the backup data will not be affected by the same disaster but is close enough to retrieve in a timely manner.

7. Disaster Recovery Plan

The Disaster Recovery Plan must define department or office procedures to restore any loss of data and equipment due to an emergency, such as power loss, fire, system failure, vandalism, natural disaster, or other occurrence. The department disaster recovery planning must start with advance preparation, including the establishment of comprehensive lists and identification of employees or non-TRS workers responsible for carrying out work after the disaster. The department manager will

work with others as necessary to compile and maintain the information below, which must be stored in multiple formats, on and off site, to be used in the event of an emergency. Depending on the nature of the work department or office and the criticality of its operation, creation of the following documents may be appropriate:

(a) Inventories
(b) Floor plans
(c) List of backup systems/data, location and contact information, and list of individuals who may access site
(d) Critical forms and supplies stocked off-site
(e) List of reliable resources for equipment replacement
(f) Contract for backup agreement for space, processing hardware and software and resources on an emergency basis, including method of retracting and utilizing data history
(g) Processing priorities pre-approved by department management
(h) System application and documentation (current copies of all applications need to be located on and off site in a secure manner); see Emergency Access Controls section below
(i) Testing and revision plans as detailed below
(j) List of job categories and/or individuals responsible for recovery of computer and other systems. Job categories may include restore operations, and/or retrieval of previously backed-up data
(k) List of all critical business partners and emergency contact information

8. Disaster Recovery Plan

The Disaster Recovery Plan must provide for continuation of critical business processes for the protection and security of ePHI even during emergency mode operations. The department or office manager will work with others as necessary to develop a critical Disaster Recovery Plan that allows for an orderly resumption of activities and system recovery to the point of failure. The plan should include an outline of the business priorities for the department, including related assumptions and a final base plan with activation criteria based on those business priorities.

9. Testing and Revision Plan

The Testing and Revision Plan must provide for routine testing of contingency plans as necessary in accordance with the department's or office's system complexity, and other factors reviewed during the risk analysis and risk management process as defined in the Information Security Manual:

(a) Each component of the department's contingency plan must be identified, evaluated, and prioritized for routine testing and adjustment or revision based on test outcomes. Test plans must be clearly documented and include instruction to notify involved parties of the test, disaster simulation, and relocation as well as a defined timeline.

(b) Different levels of testing can be performed ranging from complete mock disasters to simple desk checking of logical procedures. Any time a modification is made to a system, a corresponding plan revision should be considered and tested.

10. Disaster Recovery Strategy

The Disaster Recovery Strategy must provide for the prioritization of system applications and related data in order to support resumption of normal business and/or systems processing. To determine the order of priority for restoring systems after a disaster and ensuring that the most critical application and/or data is restored first, the department or office must consider and list computer software applications and databases in order of importance, criticality, and data sensitivity. System recovery and other contingency plan functions must be prioritized based upon this list.

11. Emergency Access Controls

Departments and offices must develop plans and procedures in concert with the IT division for accessing department level ePHI in the event of an emergency. This may involve placing new computer equipment into service, restoring data from backup devices, or creation of new logons, passwords, or other access codes. Some emergencies may result from an internal process that does not work or because an individual who has access control is not available. In these cases temporary access authorizations may be used to access systems. To be effective during an emergency, access codes must be communicated in advance to designated employees and non-TRS workers, documented in a standard manner, and securely maintained.

12. Approval of Plans

All department-level contingency plans (and all components) must be submitted to the TRS Information Security Officer, or designee, in coordination with TRS Enterprise Risk Management for review and approval.

13. Documentation and Records Retention

All decisions made and plans created pursuant to this policy must be documented and maintained securely. All documentation pursuant to this policy must be kept for a period of at least six (6) years from the date of creation of the document or the date when the document was last in effect, whichever is later.

Policy & Procedure for Data Integrity

Purpose

To outline policies and procedures for protecting ePHI from improper alteration or destruction relative to the HIPAA Security Regulations.

Applicability

This policy applies to every TRS employees and non-TRS workers who has access to or who uses ePHI and every department or office administering computer systems containing ePHI.

References

45 CFR § 164.312(c)(1) and (2)

Policy Statement

TRS shall protect ePHI from improper alteration or destruction. This responsibility resides both with the administration of TRS as well as the departments and offices directly handling or storing the data.

Procedures

1. Protecting Data Integrity

TRS must protect ePHI in its possession from improper alteration or destruction. In order to preserve the integrity of ePHI in its possession, TRS must implement a combination of policy and technical solutions. The combination includes:

(a) Policies and procedures to protect ePHI from improper alteration or destruction and to keep ePHI consistent with its source.
(b) Electronic mechanisms to confirm that ePHI has not been altered or destroyed in an unauthorized manner.

2. Integrity Controls

Integrity controls are technical safeguards to prevent or detect unauthorized alteration or deletion of ePHI and critical system and network files. Technical safeguards may include:

(a) Firewalls;
(b) Encryption;
(c) Password protection and other authentication devices;
(d) Anti-virus software; and
(e) Standards for change control, testing, documentation, approval, and rollback.

3. Department and Office Responsibilities

Each department and office directly handling or storing ePHI is responsible for maintaining internal controls to protect ePHI from improper alteration or destruction and to keep it consistent with its

source. Decisions regarding the preferred combination of processes and procedures may be made at the department or office level. However, TRS requires that collectively, the combination of solutions used by the department or office suffice to reasonably safeguard ePHI and to protect it from improper alteration or destruction. Departments and offices must document their decision-making processes on which solutions they use and all administrative solutions put in place. This information must be submitted to the Information Security Officer for approval. Documentation must be retained by the department or office for a period of at least six (6) years from the date the decision was made or the solution was last used. Departments and offices are responsible for educating all department and office members with access to ePHI on their policies, procedures, and technical solutions. Departments and offices must perform routine monitoring of the solutions chosen and policies and procedures implemented to assess the effectiveness of proving data integrity. Departments and offices must weigh the confidentiality of ePHI against its availability and integrity. Departments and offices must perform this review as needed, no less than every two (2) years.

4. Data Authentication Controls

Data authentication is the electronic process in which holders of ePHI validate data integrity, verify that the data sent is the same data that is received, and ensure the integrity of data stored and retrieved. Data authentication controls consist of the following:

(a) Database integrity – integrity checking and data recovery features which must be built into the database application

(b) Message integrity – transmitting ePHI from one place to another uses data integrity features. To ensure the protection of data transmitted over the Internet, ePHI in e-mail must be sent via the TRS secure mail. Web applications used for transmitting ePHI must incorporate secure transmission methods

(c) Procedure integrity – based on the level of risk it may be necessary to provide additional reliability in the form of redundant systems, duplicate power supplies, appropriate power conditioning and cooling systems. Regular preventive maintenance must be performed.

5. Software Controls

Systems without adequate authorization mechanisms built into the software should never be used to store or transmit ePHI. The design of TRS database systems and software used for handling ePHI should be evaluated for its ability to protect against alteration or modification; record missing or critical information; and control simultaneous updates. After database systems and software have been evaluated, if it is determined that they cannot provide the above, they should not be used to store or transmit ePHI. These systems must be upgraded or replaced.

Policy & Procedure for Person or Entity Authentication

Purpose

To provide the foundation for safeguarding systems. Authentication, or the ability to confirm that a person or entity is the one claimed, is the primary access control for validating the identity of users and monitoring their access to ePHI.

Applicability

This policy applies to all TRS employees and non-TRS workers who have access to ePHI or provide access to ePHI.

References

45 C.F.R. § 164.312(a)(2)(i)

45 C.F.R. § 164.312(d)

Policy Statement

All TRS employees and non-TRS workers shall authenticate the entity or person receiving PHI.

Procedures

1. Unique User Identification (Login)

   Each person who accesses ePHI held by TRS must perform that access using unique user identification (login). The login may be a unique name and/or number used to identify and track user identity. No TRS employee or non-TRS worker may use another member's login or allow others to use their login and/or password. The use of shared logins is prohibited when accessing ePHI. Upon notification by information owners, administrators of systems housing ePHI (or that may be used to access ePHI) are required to cancel or disable a user's account upon termination of the user's relationship with TRS or when the user no longer needs access to ePHI. Any violations of this policy must be reported to the Information Security Officer immediately.

2. Person or Entity Authentication

   Each department or office that houses ePHI must implement procedures to verify that a person seeking access to ePHI is the one claimed. ePHI housed by TRS must be protected by authentication controls on all IT resources. Valid authentication shall consist of at least a unique user login and password combination to verify user authenticity. Other authentication measures, such as cryptographic keys, tokens, smart cards, etc., may be implemented if feasible. Entity authentication may be a shared password or public key, requiring a second form of authentication. It may also be a technical mechanism built into the software itself.

Policy & Procedure for Device and Media Controls - Disposal and Reuse

Purpose

To outline the receipt, movement, and removal of hardware and electronic media that contain ePHI into and out of a facility and movement within a facility.

Applicability

All hardware and electronic media that are used for storing ePHI are subject to this policy.

References

45 C.F.R. § 164.310(d)(1)

45 C.F.R. § 164.310(d)(2)(i) – (iii)

Policy Statement

It is the responsibility of any person who uses or is required to maintain hardware or electronic media that contains ePHI to comply with this policy. This includes all TRS employees and non-TRS workers.

Procedures

1. General

These procedures govern the receipt, removal, and disposal of hardware and electronic media used for storage of ePHI at TRS, and the movement of these items within or out of a TRS facility. Electronic media includes, but is not limited to:

(a) Any electronic computing devices including laptop or desktop computers, PDAs, or any other devices that may be used to store ePHI

(b) Diskettes, compact disks (CDs), DVDs, tapes, memory sticks and all related types of removable storage devices.

2. Disposal of Hardware and Electronic Media

To ensure the protection of ePHI, all ePHI stored on hardware or electronic media must be destroyed prior to the decommissioning of the hardware or media itself. If the ePHI needs to be retained for future use, a retrievable copy can be made, however this copy must have access authorizations in place (such as password protection, etc.) to prevent unauthorized access to the ePHI. Methods for irreversibly destroying ePHI include hard drive low level formatting, disk wiping, or degaussing. Physical methods of destroying electronic media include shredding, grinding down, puncturing, shattering, or incineration. Prior to disposal, the TRS Client Service, Media Disposal Procedures should be consulted.

3. Media Reuse

Prior to device or media re-use, all ePHI stored on the device or media must be securely removed. Removal may be accomplished by disk wiping or by utilizing a reliable data destruction utility to ensure the data is non-recoverable. Caution: A typical disk reformat is not sufficient to comply with this requirement. If required, a backup copy of the stored ePHI can be made prior to re-use of the media or storage device if the ePHI is needed for future use. If a backup copy is created it must have access authorizations in place (such as password protection, etc.) to prevent unauthorized access to the ePHI. A written record of any reused or redistributed storage device or media must be created. See Inventory and Accountability section below.

4. Inventory and Accountability

TRS Client Services maintains a tracking record of the movements of hardware and electronic media used to store ePHI, including the receipt of any new hardware or electronic media storing ePHI. This record should contain, at a minimum, the name of the person responsible for the item, the location of the item, and any movement of the item. All records created pursuant to the section above must be kept by the department or office for a period of six (6) years from the date the record was created.

Policy & Procedure for Portable Media Security

Purpose

To establish guidelines for secure use of portable media and protection of any ePHI stored on portable media.

Applicability

This policy applies to the use of all types of portable devices that may be used to store ePHI. Portable media can include, but is not limited to, laptops, mobile devices such as personal digital assistants (PDAs) or other types of wireless handheld devices, USB flash drives, memory sticks, and any other portable device used to store or transport data.

References

N/A

Policy Statement

All ePHI stored on portable media shall be protected in accordance with this policy.

Procedures

1. General

If at all possible, do not store ePHI on portable media. If it is necessary to store ePHI on portable media:

(a) Password protect the device using a complex password;
(b) Encrypt the ePHI stored on the device using the TRS-provided encryption software;
(c) Store only the minimum necessary ePHI if the purpose of storing the ePHI is not for Treatment, Payment, or Healthcare Operations;

When it is no longer necessary to store the ePHI on the device:

(a) If the device will continue in use, securely erase the ePHI and the recycle bin or trash can
(b) If the device will continue to be used but none of the data stored on the device will be needed again, use a disk wiping tool to remove all traces of all data stored on the device
(c) If neither the device nor the data stored on the device will be used again, destroy the device by breaking or puncturing it
(d) Validation that the aforementioned processes has been performed by a member of the TRS Information Security department

If the device is lost or stolen, report this as soon as possible to the Information Security department.

Documentation and Records Retention

Any validation of the procedures in this policy must be documented and maintained securely. All documentation pursuant to this policy must be kept for a period of at least six (6) years from the date of creation of the document or the date when the document was last in effect, whichever is later.

Policy & Procedure for Secure Email Transmission

Purpose

To outline the procedures for handling e-mail messages containing ePHI at TRS.

Applicability

This policy applies to all TRS employees and non-TRS workers who may transmit ePHI via email.

References

45 C.F.R. § 164.312 (e)(1) and (e)(2)(ii)

Policy Statement

Anyone at TRS who communicates ePHI with recipients outside of TRS using e-mail is responsible for the protection and integrity of the data. This includes all TRS employees and non-TRS workers.

Procedures

1. General

ePHI may not be transmitted by e-mail unless the sender of the e-mail is using a secure e-mail system. TRS has implemented a secure messaging system which is specifically designed for the transmission of e-mail messages containing ePHI and other sensitive information. Full documentation and instructions for the use of the TRS secure e-mail system can be found on the IT website. The TRS secure e-mail system must be used when communicating ePHI via e-mail outside of the private network belonging to TRS and its major affiliates. E-mails sent within TRS or from TRS to a major affiliate are already protected and do not need to be sent via the secure e-mail system. TRS employees and non-TRS workers who need to send ePHI or other sensitive information via e-mail and are not on the TRS network must use a secure e-mail system that has the following features:

(a) Transmission Security. The message cannot be intercepted by someone other than the intended recipient while the message is in transmission. Transmission security can be accomplished by the use of encryption.

(b) Mechanism to Authenticate. The recipient of the message must have the ability to know that the content of the message has not been altered during transmission. This must be built into the e-mail system in use.

(c) Updated anti-virus protection must be in place on any TRS computing device either sending or receiving e-mail. Updated anti-virus protection must also be in place on the e-mail servers and at the e-mail gateways.

Policy & Procedure for Remote Access Security

Purpose

To provide general guidelines to ensure security of ePHI on home computers and when accessing ePHI on the TRS network from home.

Applicability

This policy applies to TRS employees and non-TRS workers, who connect to the TRS network systems, applications and data, including but not limited to applications that contain ePHI, from a remote location (the "Remote Worker"). This policy applies to computers owned by TRS and computers owned by the TRS employees and non-TRS workers.

References

Remote Access Security Policy

Remote Work Policy

Policy Statement

Authorized TRS employees and non-TRS workers will be allowed access to the TRS Network through the use of equipment owned by or leased to TRS, or through the use of the Remote Worker's personal computer system in accordance with the Remote Access Security Policy. All TRS employees and non-TRS workers who access ePHI on the TRS network from a remote location shall follow this policy.

Procedures

1. Remote Access to the TRS Network

Before connecting to the TRS network via remote access, the Remote Worker must:

(a) Be approved for remote access connections in accordance with the Remote Access Security Policy and Remote Work Policy. Remote accessis strictly controlled and made available based on a defined business need, at the discretion of the TRS employee's and non-TRS worker's manager.

(b) Install and keep up-to-date the TRS standard anti-virus software, or something compatible if using a home computer, to prevent the spread of malware (viruses/Trojans, etc.);

(c) Apply critical security patches for operating systems and applications and keep patches up-to-date;

(d) Install anti-spyware software, keep it up-to-date, and run software on a regular basis, no less than monthly; Care must be taken when accessing web sites; many websites harbor malware. Anti-spyware software should be run after leaving a site whose security may be suspect;

(e) software approved by Information Security Officer may be installed on a computer Only owned by TRS;

(f) Install and enable a firewall software application.

(g) If the home computer is part of a home network, Remote Workers are not permitted to download ePHI to the computer, unless it is necessary to fulfill their job responsibilities. Home networks introduce greater risk of unauthorized access to the data. If the home network is a wireless home network, Remote Workers must ensure that the latest wireless security is in place. Currently that means installing WPA (Wi-Fi Protected Access) on the home computer. Wireless networks set up with default wireless encryption are insecure.

2. Method of Remote Access to TRS Network

There are three ways to access the TRS network remotely through a TRS-owned device, employee-owned device, or via a virtual machine (VM).

(a) FortiClient allows your device to connect to the TRS network and operate very similarly to when you're in the office

(b) Web VPN only provides the ability to remote desktop back to your TRS-owned device.

(c) You can access the TRS network via a Virtual Machine (VM)

3. Download of ePHI to Home Computers

Extra care must be taken if ePHI is downloaded or saved on home computers.

(a) ePHI should not be downloaded or saved on home computers or other personal media without prior written approval from the Remote Worker's manager.

(b) ePHI stored on the home computer must be encrypted to protect against unauthorized access.

(c) If ePHI must be transmitted across the Internet via e-mail, use of the TRS e-mail system and secure e-mail procedures are required.

(d) If ePHI must be transmitted across the Internet via any means other than e-mail, the ePHI must be encrypted prior to transmission or a secure connection must be made.

(e) When the ePHI is no longer needed on the home computer, it must be completely removed from the computer. After securely wiping the files, the Windows Recycle Bin or Macintosh Trashcan must also be securely emptied.

(f) If the home computer stores ePHI and is stolen or accessed by a third-party, the user must notify the TRS Information Security Officer as soon as the theft or access is discovered.

(g) If the home computer contains or contained ePHI and becomes non-functional or is to be replaced, The Remote Worker must notify TRS Information Security Officer. The ePHI must be permanently destroyed prior to disposing of the computer. If the computer is functional, use a disk wiping tool to permanently destroy the ePHI. If the computer is non-functional, remove the hard drive and destroy it either by smashing or puncturing it.

4. Printing and Storage

TRS discourages Remote Workers from using or printing paper documents that contain PHI. The ability to print a document to a remote printer is not supported without the organization's approval. Documents printed that contain confidential business or ePHI shall be managed in accordance with TRS's Confidentiality and HIPAA Policies and Procedures. The following equipment and environment is required in order to print ePHI from a remote location:

(a) Paper Shredder
(b) Secure office environment isolated from visitors and family
(c) A lockable file cabinet or storage device to secure documents when unattended

5. Remote Security

Remote Workers must take necessary precautions to secure all of TRS's equipment and proprietary information in their possession.

(a) Remote users shall lock the workstation and/or system(s) when unattended so that no other individual is able to accessany ePHI or organizationally sensitive information.
(b) Remote Workers shall automatically be disconnected from the TRS's network when there is no recognized activity for 15 minutes
(c) It is the responsibility of Remote Workers to ensure that unauthorized individuals do not access the network. At no time will any Remote user provide (share) their user name or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.

6. Monitoring Remote Access

(a) TRS maintains logs of all activities performed by Remote Workers while connected to TRS's network. The Information Security Department will review this documentation and/or use automated intrusion detection systems to detect suspicious activity. Accounts that have shown no activity for 30 days will be disabled.
(b) With appropriate notice or given cause, management reserves the right to have a qualified person visit the home office environment or to make inquiries as to the status of the environment. Reasonable notification will be at minimum 24 hours, except in cases of emergency.

.

Policy & Procedure for Employee Training & Corrective Action

Purpose

The Privacy Regulations require that all TRS employees and non-TRS workers be educated and trained as to the appropriate manner of handling PHI in order to carry out their job functions and that those who fail to comply with the Plan's privacy policies and procedure be appropriately sanctioned.

References

Reference: 45 C.F.R §164.530(b)

Reference: 45 §164.530(b)(2)(ii)

Reference: 45 §164.530(e)(1)

Policy

TRS will train all TRS employees and non-TRS workers on the importance of privacy and TRS' policies and procedures with respect to PHI, as necessary and appropriate for TRS employees and non-TRS workers to carry out their function within the Plan.

Procedure

1. Identifying Trainees and Timing of Training

The Chief Compliance Officer, in coordination with the Information Security Officer and the Privacy Officer, will be responsible for identifying TRS employees and non-TRS workers who perform a function for the Plan involving the use of PHI. The Chief Compliance Officer will ensure that TRS employees and non-TRS workers receive training according to the following schedule:

(a) to each new TRS employee or non-TRS worker within 30 days after the person joins TRS or is assigned to TRS; and

(b) to each TRS employee or non-TRS worker whose functions are affected by a material change in the policies or procedures, within a reasonable period of time after the material change becomes effective, and no less frequently than annually.

The Plan will provide additional training as to the Plan's Policies and Procedures to any individual employee or Business Associate of the Plan, upon request.

2. Content of Training.

Training will involve an overview of TRS' obligations under the Privacy Regulations and the TRS' Policies and Procedures that are applicable to the individuals being trained. The training may be presented in written, electronic, or verbal form.

3. Documentation of Training

Organizational Excellence will document the content, date, and attendance at each of the training sessions as described above and will retain such documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

4. Corrective Actions

TRS employees and non-TRS workers who use or disclose an individual's PHI in violation of the training provided, the Privacy Regulations, or these Policies and Procedures will be subject to corrective actions that will be consistent with the nature of the violation. Consistent with the TRS Corrective Action Policy, action may include, but is not limited to, verbal and written notice, suspensions, and termination. Corrective actions will be imposed by the Executive Director in consultation with the Chief Compliance Officer and Privacy Officer. TRS Compliance will document any sanctions that are imposed.

Glossary

Breach

a) The acquisition, access, use, or disclosure of Protected Health Information in a matter not permitted under the Privacy Regulations which compromises the security or privacy of the Protected Health Information.

b) *Breach* excludes:

   a) Any unintentional acquisition, access, or use of Protected Health Information by a TRS employee and non-TRS worker or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Regulations.

   b) Any inadvertent disclosure by a person who is authorized to access Protected Health Information at a Covered Entity or Business Associate to another person authorized to access Protected Health Information at the same Covered Entity or Business Associate, or Organized Health Care Arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Regulations.

   c) A disclosure of Protected Health Information where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

c) An acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the Privacy Regulations is presumed to be a Breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors:

   a) The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification;

   b) The unauthorized person who used the Protected Health Information or to whom the disclosure was made;

   c) Whether the Protected Health Information was actually acquired or viewed; and

   d) The extent to which the risk to the Protected Health Information has been mitigated.

Business Associate

1. Except as provided in paragraph (4) of this definition, *Business Associate* means, with respect to a Covered Entity, a person who:

   a) On behalf of such Covered Entity or of an Organized Health Care Arrangement in which the Covered Entity participates, but other than in the capacity of a member of the

Workforce of such Covered Entity or arrangement, creates, receives, maintains, or transmits Protected Health Information for a function or activity regulated by the Privacy Regulations, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, Patient Safety Activities, billing, benefit management, practice management, and repricing; or

b) Provides, other than in the capacity of a member of the Workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an Organized Health Care Arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of Protected Health Information from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

2. A Covered Entity may be a Business Associate of another Covered Entity.
3. Business Associate includes:
   a) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to Protected Health Information to a Covered Entity and that requires access on a routine basis to such Protected Health Information.
   b) A person that offers a personal health record to one or more individuals on behalf of a Covered Entity.
   c) A subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of the Business Associate.
4. Business Associate does not include:
   a) A Health Care Provider, with respect to disclosures by a Covered Entity to the Health Care Provider concerning the Treatment of the individual.
   b) A plan sponsor, with respect to disclosures by a Group Health Plan (or by a Health Insurance Issuer or HMO with respect to a Group Health Plan) to the plan sponsor.
   c) A government agency, with respect to determining eligibility for, or enrollment in, a government Health Plan that provides public benefits and is administered by another government agency, or collecting Protected Health Information for such purposes, to the extent such activities are authorized by law.
   d) A Covered Entity participating in an Organized Health Care Arrangement that performs a function or activity as described by paragraph (1)(a) of this definition for or on behalf of such Organized Health Care Arrangement, or that provides a service as described in paragraph (1)(b) of this definition to or for such Organized Health Care Arrangement by virtue of such activities or services.

Business Associate Agreement

The contract between TRS and a Business Associate established to protect Personal Health Information (PHI).

Chief Compliance Officer

The Chief Compliance Officer (CCO) of a company is the officer primarily responsible for overseeing and managing regulatory compliance issues within an organization. Heather Traeger is the Chief Compliance Officer.

Covered Entity

1. A Health Plan.
2. A Health Care Clearinghouse.
3. A Health Care Provider who transmits any Health Information in electronic form in connection with a transaction covered by this subchapter.

Data Aggregation

With respect to PHI created or received by a Business Associate in its capacity as the Business Associate of a Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the Health Care Operations of the respective covered entities.

Data Use Agreement

A data use agreement (DUA) is an agreement required by the HIPAA Privacy Regulations between TRS and a person or entity that receives a "limited data set" from TRS.

Genetic Information

Genetic Information means:

1. Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:
   a) The individual's genetic tests;
   b) The genetic tests of family;
   c) The manifestation of a diseased or disorder in family members of such individual; or
   d) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.
2. Any reference to Genetic Information concerning an individual or family member of an individual shall include the Genetic Information of:
   a) A fetus carried by the individual or family member who is a pregnant woman; and

b) Any embryo legally held by an individual or family utilizing an assisted reproductive technology.

3. Genetic Information excludes information about the sex and age of any individual.

Health Care

Care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse

A public or private entity, including a billing service, repricing company, community health management information system or community Health Information system, and "value-added" networks and switches, that does either of the following functions:

1. Processes or facilitates the processing of Health Information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
2. Receives a standard transaction from another entity and processes or facilitates the processing of Health Information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations

Any of the following activities of a Covered Entity to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; Patient Safety Activities; population-based activities relating to improving health or reducing Health Care costs, protocol development, case management and care coordination, contacting of Health Care Providers and patients with information about Treatment alternatives; and related functions that do not include Treatment;
2. Reviewing the competence or qualifications of Health Care professionals, evaluating practitioner and provider performance, Health Plan performance, conducting training programs in which students, trainees, or practitioners in areas of Health Care learn under

supervision to practice or improve their skills as Health Care Providers, training of non-Health Care professionals, accreditation, certification, licensing, or credentialing activities;

3. Underwriting, enrollment premium rating, and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for Health Care (including stop-loss insurance and excess of loss insurance), provided that the Health Plan receiving Individually Identifiable Health Information does not disclose such information if the insurance or benefits are not placed with it.
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities of the entity, including, but not limited to:
   (a) Management activities relating to implementation of and compliance with the requirements of this subchapter;
   (b) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;
   (c) Resolution of internal grievances;
   (d) The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that, following such activity, will become a Covered Entity and due diligence related to such activity; and
   (e) Creating de-identified Health Information or a limited data set, and if current policy is amended to allow fundraising, fundraising for the benefit of the Covered Entity.
   (f) Use of an individual's PHI in pension administration in the furtherance of the purpose for which the PHI was provided to the Plans, such as processing an application for disability retirement or reviewing a springing POA.

Health Care Provider

A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for Health Care in the normal course of business.

Health Information

Any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a Health Care Provider, Health Plan, Public Health Authority, employer, life insurer, school or university, or Health Care Clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of Health Care to an individual; or the past, present, or future Payment for the provision of Health Care to an individual.

Health Insurance Issuer (as defined in section 2791(b)(2) of the Public Health Service Act, 42 U.S.C. 300gg–91(b)(2) and used in the definition of Health Plan in this section)

An insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a Group Health Plan.

Health Maintenance Organization (HMO) (as defined in section 2791(b)(3) of the Public Health Service Act, 42 U.S.C. 300gg–91(b)(3) and used in the definition of Health Plan in this section)

A federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health Plan

An individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg–91(a)(2)).

1. Health Plan includes the following, singly or in combination:
    a) A Group Health Plan, as defined in this section.
    b) A Health Insurance Issuer, as defined in this section.
    c) An HMO, as defined in this section.
    d) Part A or Part B of the Medicare program under title XVIII of the Act.
    e) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
    f) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
    g) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
    h) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
    i) The Health Care program for active military personnel under title 10 of the United States Code.
    j) The Veterans Health Care program under 38 U.S.C. chapter 17.
    k) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).

l) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

m) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

n) An approved State child Health Plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

o) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.

p) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

q) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

2. Health Plan excludes:

a) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg–91(c)(1); and

b) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):

i. Whose principal purpose is other than providing, or paying the cost of, Health Care; or

ii. Whose principal activity is: (A) the direct provision of Health Care to persons; or (B) the making of grants to fund the direct provision of Health Care to persons.

HITECH Act

The Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, as amended.

Individual

The person who is the subject of PHI.

Individually Identifiable Health Information

Information that is a subset of Health Information, including demographic information collected from an individual, and:

1. Is created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of Health Care to an individual; or the past, present, or future Payment for the provision of Health Care to an individual; and
    a) That identifies the individual; or
    b) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information Security Officer

The Information Security Officer is the officer responsible for developing and implementing an information security program, which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats.

Organized Health Care Arrangement

Any of the following arrangements:

1. A clinically integrated care setting in which individuals typically receive Health Care from more than one Health Care Provider.
2. An organized system of Health Care in which more than one Covered Entity participates and in which the participating covered entities:
    a) Hold themselves out to the public as participating in a joint arrangement; and
    b) Participate in joint activities that include at least one of the following:
        i. Utilization review, in which Health Care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
        ii. Quality assessment and improvement activities, in which Treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
        iii. Payment activities, if the financial risk for delivering Health Care is shared, in part or in whole, by participating covered entities through the joint arrangement and if Protected Health Information created or received by a Covered Entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
3. A Group Health Plan and a Health Insurance Issuer or HMO with respect to such Group Health Plan, but only with respect to Protected Health Information created or received by such Health Insurance Issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such Group Health Plan.
4. A Group Health Plan and one or more other Group Health Plans each of which are maintained by the same plan sponsor.

5. The Group Health Plans described in paragraph 4 and Health Insurance Issuers or HMOs with respect to such Group Health Plans, but only with respect to Protected Health Information created or received by such Health Insurance Issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such Group Health Plans.

Patient Safety Activities

The following activities carried out by or on behalf of a Patient Safety Organization or a provider:

1. Efforts to improve patient safety and the quality of Health Care delivery;
2. The collection and analysis of patient safety work product;
3. The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices;
4. The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk;
5. The maintenance of procedures to preserve confidentiality with respect to patient safety work product;
6. The provision of appropriate security measures with respect to patient safety work product;
7. The utilization of qualified staff; and
8. Activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system.

Patient Safety Organization

A private or public entity or component thereof that is listed as a patient safety organization ("PSO") by the Secretary pursuant to 42 C.F.R. Part 3. A Health Insurance Issuer or a component organization of a Health Insurance Issuer may not be a PSO. See also the exclusions in § 3.102 of this part.

Payment

1. The activities undertaken by:
   a) A Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Health Plan; or
   b) A Health Care Provider or Health Plan to obtain or provide reimbursement for the provision of Health Care; and
2. The activities in paragraph (1) of this definition relate to the individual to whom Health Care is provided and include, but are not limited to:

a) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
b) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
c) Billing, claims management, collection activities, obtaining Payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related Health Care data processing;
d) Review of Health Care services with respect to medical necessity, coverage under a Health Plan, appropriateness of care, or justification of charges;
e) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and
f) disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
    i. Name and address;
    ii. Date of birth;
    iii. Social security number;
    iv. Payment history;
    v. Account number; and
    vi. Name and address of the Health Care Provider and/or Health Plan.

Plan

The Teacher Retirement System of Texas ("TRS") administers three trust funds for the benefit of active and retired public school teachers in the State of Texas: (a) the Pension Trust Fund; (b) the TRS-ActiveCare Trust Fund; and (c) the TRS-Care Trust Fund. The Pension Trust Fund provides retirement benefits and death benefits to eligible retirees, including benefits based on a member's disability. Disability determinations require the use of PHI. TRS-ActiveCare provides medical and prescription drug benefits to eligible active public school employees and their eligible dependents; these employees must be employed by participating entities in TRS-ActiveCare. TRS-Care provides medical and prescription drug benefits to eligible retirees and their eligible dependents; these retirees have been employed by public school districts and charter schools in the State of Texas during their teaching careers. Each of these programs and their respective trust funds will be referred to in these Policies and Procedures as a "Plan" and collectively they will be referred to as the "Plans."

Plan Administrator

Teacher Retirement System of Texas

Plan Sponsor

Teacher Retirement System of Texas

Privacy Officer

The privacy officer oversees the development, implementation, maintenance of, and adherence to privacy policies and procedures regarding the safe and handling of protected health information (PHI) in compliance with federal and state HIPAA Privacy and Security Regulations. W. Clarke Howard is the HIPAA Privacy Officer.

Privacy Regulations

The Standards for the Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164, as amended.

Protected Health Information or PHI

Individually identifiable health or Genetic Information:

1. Except as provided in paragraph (2) of this definition, that is:
   a) Transmitted by electronic media;
   b) Maintained in any medium described in the definition of electronic media; or
   c) Transmitted or maintained in any other form or medium.
2. PHI excludes Individually Identifiable Health Information in:
   a) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g;
   b) Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of Treatment to the student, and are not available to anyone other than persons providing such Treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice as described at 20 U.S.C. 1232g(a)(4)(B)(iv);
   c) Employment records held by a Covered Entity in its role as employer; and
   d) Information about an individual who has been deceased for 50 years.

Secretary

The Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Security Regulations

The Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Parts 160 and 164, as amended.

State

One of the following:

1. For a Health Plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such Health Plan.
2. For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.

Subcontractor

A person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the Business Associate's Workforce.

Third-Party Administrator

A person or entity chosen by the Plan or the Plan Sponsor to assist the Plan with identified administrative functions such as claims administration or adjudication. Each Third-Party Administrator is a Business Associate of the Plan. Examples include health plan administrators and pharmacy benefit managers.

Treatment

The provision, coordination, or management of Health Care and related services by one or more Health Care Providers, including the coordination or management of Health Care by a Health Care Provider with a third party; consultation between Health Care Providers relating to a patient; or the referral of a patient for Health Care from one Health Care Provider to another.

Unsecured Protected Health Information or Unsecured PHI

Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services in the guidance issued under the HITECH Act.

Appendix

Security Incident Log Template

Date and Time Reported:

_____

Reported by (name of person filling out report):

_____

Reported to (name of person receiving report):

_____

Date and Time of Incident:

_____

Category of Incident:

_____

Contact information for system owner:

Name:

_____

_____

Department:

_____

_____

Location:

_____

_____

Phone Numbers:

_____

__

Device serial number and model number:

_____

Computer name:

_____

MAC address:

_____

IP address:

_____

Witnesses/other parties of interest:

_____

Who will take the lead in coordinating the investigation?

_____

Members of investigating team:

_____

_____

____

Summary of Incident (attach sheet if necessary):

_____

_____

_____

_____

_____

Is there sensitive data involved? Explain:

_____

_____

_____

_____

Is the incident over? Θ Yes Θ No

If the incident is likely to result in criminal or civil legal action,

Θ Preserve the evidence and halt/isolate the incident as appropriate.

What is the risk? Who will be impacted (division, business unit)?

_____

_____

_____

_____

Outline the steps to be taken:

_____

_____

_____

_____

_____

_____

Security Incident Log:

_____

_____
_____
_____
_____

_____

At conclusion of the investigation, were the individuals affected by the incident notified?

Θ Yes Θ No (If yes, attach a copy of that correspondence.)

Has a final report of the incident, investigation, response, and remediation been written?

Θ Yes Θ No (Attach a copy of the report.)