


**Department of Finance & Administration  
Division of TennCare**

<b>Policy Number: PRIV 013</b>	
<b>Policy Subject: Privacy, Security, and Confidentiality Training Policy</b>	
<b>Printed Name: Andrei Dumitrescu</b>	<b>Effective Date: 10/17/2023</b>
<b>Position: Chief Compliance and Privacy Officer</b>	
<b>Signature:</b> 	

**PURPOSE**

This policy addresses how the Division of TennCare (TennCare) provides training of workforce members in the proper access, use, and safeguarding of information, including public, sensitive, and restricted access information as defined in the Data and Information Systems Classification Policy. The information may be regarding its programs, enrollees, or partners, and it can include Personally Identifiable Information (PII), Protected Health Information (PHI) including electronic Protected Health Information (ePHI), Social Security Administration provided information (SSA information), and Federal Tax return Information (FTI).

**SCOPE**

This policy covers all TennCare information systems used, managed, provided, or operated by the state or a vendor, contractor or another organization acting on behalf of TennCare. The policy applies to all TennCare employees, consultants, contractors, and other persons who are under the direct or indirect control of TennCare and who access TennCare systems. For the purposes of this policy, all persons are described as workforce members.

**POLICY**

TennCare shall provide appropriate training to all TennCare employees on its policies and procedures related to the privacy, security, and confidentiality (PSC) of information created, maintained, used, accessed, or transmitted regarding its benefit population. Additionally, TennCare shall provide specialized training as necessary to employees based on their access to public, sensitive, and restricted access information.

## **TRAINING FOR TENNCARE EMPLOYEES**

As part of the onboarding process, prior to system and information access, all personnel must acknowledge the contents of the Acceptable Use Policy (AUP), which includes details regarding treatment of confidential information. This is followed by new hire privacy, security, and confidentiality (PSC) training within no more than two (2) quarters of hire date. Every employee of TennCare is also required to complete an annual renewal and recertification of the awareness training.

The PSC training includes a variety of topics, from proper access, use, disclosure, and transmission of information, to recognizing and reporting indicators of threats, penalties for misuse of information, and incident reporting and resolution. Other specific topics covered in the PSC training include:

- a) insider threat, phishing, and malware awareness and recognition;
- b) physical security measures;
- c) desktop security;
- d) appropriate use of wireless networks;
- e) credential and password security;
- f) proper data storage, retention, and disposal; and
- g) secure transmittal of sensitive information (via email, fax, and mail).

The TennCare Privacy Office shall periodically review and revise all TennCare provided training materials to ensure the information presented is in compliance with current federal and state privacy, security, and confidentiality laws and regulations.

## **TRAINING FOR TENNCARE CONTRACTORS & AGENTS**

As part of the onboarding process, and prior to system and information access, all contractor staff must acknowledge the contents of the Acceptable Use Policy (AUP), which includes details regarding treatment of confidential information. Contractor staff must also complete any additional trainings required by TennCare prior to being granted access to sensitive or restricted data.

TennCare contractors are required to provide their employees appropriate training on privacy, security, and confidentiality of information created, maintained, used, accessed, received, or transmitted regarding TennCare programs and its benefit population.

Similar to the state employee training, the contractor's security and privacy awareness training should include a variety of topics including:

- a) proper access, use, disclosure, and transmission of information;
- b) recognizing and reporting indicators of threats;

- c) penalties for misuse of information; and
- d) incident reporting and resolution.

Other relevant topics which should be covered training may include:

- a) insider threat, phishing, and malware awareness and recognition;
- b) physical security measures;
- c) desktop security;
- d) appropriate use of wireless networks;
- e) credential and password security;
- f) proper data storage, retention and disposal; and
- g) secure transmittal of sensitive information (via email, fax and mail).

Through contractual requirements they are to provide necessary training as appropriate to contractor staff based on their access to public, sensitive, and restricted access information, such as FTI, SSA, PII, and PHI. For public, sensitive, and restricted access information that requires contractor staff to receive the same awareness-training as TennCare employees, TennCare shall make the specific compliance training materials available to the contractor's employer. Contractors shall maintain all awareness-training records for their staff and make them available to TennCare upon request, or as otherwise required.

## **TRAINING FOR ROLES WITH SIGNIFICANT INFORMATION SECURITY AND PRIVACY ROLES**

Certain individuals or groups may require role-specific training based on their access roles or particular types of data. This may consist of training based upon the type of data handled in addition to system-specific role-based training. This training will be conducted by the TennCare Security Office and coordinated with the Privacy Office and the Business and System Owners to ensure that all roles handling data receive appropriate training.

## **DISCUSSION & LEGAL BASIS**

Federal and state laws and regulations require that workforce members who have access to state or federally regulated information must be trained on, be aware of, and understand the requirements for protecting the privacy, security, and confidentiality of the information or data. The workforce shall receive the appropriate training, which may include PSC awareness training, role-based, and specialized training, by required compliance dates.

All workforce members who must access, use or disclose sensitive or restricted access information such as PII, PHI, FTI, or SSA as part of their job duties, must receive appropriate training in compliance with applicable regulatory requirements. Workforce members are required to participate in an annual renewal and recertification of training. Workforce members are required

to attest to their receipt of training and acknowledge the rules of behavior associated with use of sensitive or restricted access information.

TennCare shall document that all workforce members who must access, use, or disclose sensitive or restricted access information, such as PII, PHI, ePHI, FTI, or SSA information, as part of their job duties have received appropriate training in compliance with applicable laws.

## **PROCEDURE**

- As part of the onboarding process, prior to system access, all personnel must acknowledge the contents of the Acceptable Use Policy (AUP), which includes treatment of confidential information.
- Within no more than two (2) quarters of hire date, employees are required to complete TennCare new hire PSC training.
- As appropriate: additional specialized/role-based training(s), geared toward the access to state or federally regulated data/job functions of the employee, are required.
- Newly hired TennCare employees will receive an email invitation from the Privacy Office to attend the new hire training. Employees must attend the new hire training as scheduled, or contact their supervisor and/or the Privacy Office to arrange for attendance on alternate dates.
- All TennCare employees shall receive an email invitation from the Privacy Office to complete annual training. Employees must complete the annual training within the time frame indicated or contact their supervisor and/or the Privacy Office to arrange for alternate timeframes based on extenuating circumstances, such as long-term medical leave.
- To ensure proper documentation, TennCare shall document the attendance and completion of training.
  - For any in-person training:
    - i. Training participants shall be required to fill out a sign-in sheet to verify attendance at the training;
    - ii. Optional evaluation may be submitted upon completion of the training session;
    - iii. Participants may be required to submit a Statement of Understanding counter-signed by his/her supervisor.
  - For any web-based training:
    - i. The TennCare Privacy Office shall use tracking tools as available to track progress and completion of training for each participant.
    - ii. Participants may be required to submit a Statement of Understanding counter-

signed by his/her supervisor or to complete an electronic acknowledgement of completion.

- The TennCare Privacy Office shall maintain a training database signifying all participants' satisfactory attendance and completion of each required stage of training. Training records shall be retained for a minimum period of five (5) years.
- Upon notification by an employee's supervisor, and in consultation with TennCare Human Resources, the TennCare Privacy Office shall schedule the employee for any necessary additional training as job duties require or are affected by a material change in the job plan or as otherwise determined necessary or appropriate. The TennCare Security Office will be consulted where appropriate.
- Failure to attend three (3) consecutive scheduled in-person training sessions or timely completion of web-based training without prior approval shall be grounds for referral to the Director of Administration & Talent Management for appropriate sanctions.

## DEFINITIONS

**Enrollee:** An individual currently enrolled in any category of State of Tennessee's Medicaid program (TennCare) and Children's Health Insurance Program (CHIP, known as CoverKids in Tennessee) or in any Tennessee federal Medicaid waiver program pursuant to Sections 1115 or 1915 of the Social Security Act. For purposes of TennCare privacy policies, the term "enrollee" may also be used to reference an individual who was previously an enrollee during a period for which there is a privacy request or compliance inquiry.

**Federal Tax Information (FTI) and Return Information:** FTI is any return or return information received by TennCare from the Internal Revenue Service (IRS) or secondary source, such as Social Security Administration. FTI includes any information created by TennCare that is derived from return or return information. A return is any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the Internal Revenue Code and filed with the IRS by, on behalf of, or with respect to any person or entity. Return information is any information collected or generated by the IRS with regard to any person's liability or possible liability under the Internal Revenue Code.

**Social Security Administration (SSA) provided information:** Records, information, or data received from specific SSA feeds, potentially including:

- a) names;
- b) SSNs;
- c) addresses;

- d) amounts and other information related to SSA benefits; and
- e) earnings information for individuals.

This data is subject to computer matching and privacy protection agreements between TennCare and SSA which set forth the terms and conditions for the use, disclosure, and disposition of such data.

**Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

**The Privacy Act of 1974:** A United States federal law, enacted December 31, 1974, and codified at 5 U.S.C. § 552a which establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information.

**Protected Health Information (PHI):** Information that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium, including demographic information that identifies or may be used to identify an individual and 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 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.

**Electronic Protected Health Information (ePHI):** Electronic health information (ePHI) is any PHI that is created, stored, transmitted, or received electronically.

**Workforce Members:** TennCare employees, contractors, and vendors, including off-site workforce personnel who have access to TennCare data, except to the extent a workforce member is employed by an agency of the State of Tennessee other than TennCare that has implemented its own PSC training policy.

## **OFFICE OF PRIMARY RESPONSIBILITY**

The Division of TennCare Privacy Office, Office of General Counsel (OGC)

## **REFERENCES:**



5 U.S.C. § 552a

45 C.F.R. § 160.103

42 C.F.R. § 431.305

45 C.F.R. § 164.308(a)(5)(i)

26 U.S.C.A. § 6103(P)(4)(D)

IRS Publication 1075