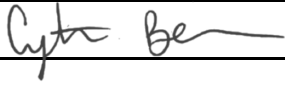


Department of Finance & Administration Division of TennCare

Policy Number: PRIV 004	
Policy Subject: Policy for Workforce Sanctions Addressing Information Security and Privacy Violations	
Approved by: Cynthia Beeler	Effective Date: 9/25/2024
Position: Chief Privacy and Compliance Officer	
Signature: 	

I. PURPOSE

The purpose of this policy is to describe how the Division of TennCare (TennCare) will address and determine appropriate sanctions/corrective action for information security and privacy violations, including unauthorized use or disclosure of confidential, sensitive, or restricted data by TennCare workforce members, to include Protected Health Information as regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

II. 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.

III. POLICY:

In instances where there is unauthorized or inappropriate receipt, use, or disclosure of confidential, sensitive, or restricted data by TennCare personnel, TennCare will take appropriate action as required by applicable federal and state privacy laws and regulations. In documented instances of unauthorized access, use, or disclosure of confidential, sensitive, or restricted data, TennCare will appropriately investigate and sanction the workforce member, if necessary, up to and including termination from employment. The workforce member may also be subject to federal and/or state criminal or civil legal action resulting in additional penalties. Such sanctions are part of TennCare's compliance with HIPAA and federal and state privacy laws and regulations.

IV. DEFINITIONS:

Any term that is capitalized in this policy without a definition in the section below is to be defined as it appears in HIPAA.

Workforce: Workforce members includes employees, professional staff, contractors who are directly assigned to projects and general support contractors of TennCare's vendors, and other persons whose conduct, in the performance of their work, is under the direct control of TennCare, whether or not they are paid by TennCare.

Confidential Record: Any record that is protected from unauthorized public disclosure under the Tennessee Public Records Act (TPRA), including but not limited to: documents containing TennCare proprietary information; system and network security related documents; privileged, legal, Audit and Human Resources documents; and personally identifiable information relating to members of TennCare workforce.

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

Encryption: The process of converting data by scrambling into a form that cannot easily be read without knowledge of the conversion mechanism (often called a key). This increases the security of an electronic Transmission.

Enrollee: Those currently enrolled in any category of TennCare Medicaid and TennCare Standard, including an individual eligible for and enrolled in the TennCare Program or in any Tennessee federal Medicaid waiver program pursuant to Sections 1115 or 1915 of the Social Security Act; and, for purposes of TennCare Privacy policies, the term may also be used to reference one who was previously an enrollee during a period for which there is a privacy request or compliance inquiry.

HIPAA: The Health Insurance Portability and Accountability Act of 1996 and for which administrative simplification, privacy, and security regulations are codified at 45 Code of Federal Regulations, Parts 160-164.

Incidental Disclosure: A term of art used to describe inadvertent or uncalculated releases of information that may occur coincidentally during TennCare operations, such as when a person overhears a nearby TennCare workforce member discuss health information on the phone.

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.

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 health or the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. *See* 45 C.F.R. § 160.103.

Sensitive or Restricted Data: Information that is classified as sensitive or restricted data in the Data and Information Systems Classification Policy, including but not limited to PII, PHI, TBI, CJIS, FTI, Confidential Records, or SSA data.

User: A member of the TennCare workforce who has responsibility for their individual use of and access to TennCare resources, such as the computer and information in the Medicaid management information system.

V. DISCUSSION & LEGAL BASIS:

This policy will be interpreted to be consistent with State of Tennessee Security Policies, including but not limited to, the Division of TennCare “Acceptable Use of TennCare Resources Policy” and “Acknowledgement of Policy.” This includes any amendments, supplements, or replacements to such security policies.

Incidental Disclosures are not generally within the scope of this policy and are not subject to sanction in most circumstances. HIPAA contemplates that such disclosures may sometimes occur in the course of routine treatment, payment, or healthcare operations. TennCare does not expect such disclosures to be reported if they occur in the normal course of permissible health care operations and TennCare uses means appropriate to the circumstances to limit the disclosures.

VI. PROCEDURES:

VI.1 General Procedure

1. The TennCare Privacy Office is responsible for receiving, logging, and investigating incidents of possible unauthorized uses or disclosures of confidential, sensitive, or restricted data. The Chief Privacy Officer will supervise and respond to the incident on behalf of TennCare as necessary.

2. In the event a report of unauthorized disclosure by TennCare personnel suggests workforce misconduct, the Privacy Office shall initiate a privacy investigation of the disclosure. Privacy Office staff may also communicate with an employee’s direct supervisor and/or refer the investigation to the TennCare Internal Audit, Human Resources, other TennCare departments, or other State agencies as appropriate, while maintaining confidentiality to the extent that is possible during the investigation.

3. All documents and investigation communications shall be treated as confidential to persons outside TennCare and shall be subject to both legal privilege and the relevant provisions of HIPAA. However, in some cases, per T.C.A. 47-18-2017, notification of the individual whose personal information was

accessed or disclosed shall be required.

4. The TennCare Privacy Office will log the use or disclosure in a manner consistent with statutes or policies requiring it. If the release suggests a pattern which may require review or intervention by the TennCare Information Systems staff or System Technology Solutions (STS) (a division of the Department of Finance and Administration) the Privacy Office will notify the TennCare Chief Information Security Officer and/or the Chief Information Officer (CIO), the General Counsel, and the Human Resources Director, as applicable.

5. Upon completion of the privacy investigation, the Privacy Office will notify the appropriate Department Executives if inappropriate conduct by TennCare workforce is suspected. If necessary, the Privacy Office will then refer the matter to TennCare Human Resources for further investigation and disciplinary action. Vendor, Contractor, or Partner Employees are subject to referral to related management and TennCare stakeholders for corrective action.

VI.2 Categorization of Privacy and Security Violations

The following privacy violation categories have been developed to provide TennCare with guidance for consistency in reporting and investigating privacy and security events, and applying sanctions/corrective action to workforce members. The examples below are meant to provide illustrative guidance and are not meant to be inclusive of every scenario. Each investigation is reviewed on an individual basis. To the extent that a violation could fall into several categories, the intent or suspected intent behind the violation is the determining factor in assigning a category.

1.1 Category 1: Suspected accidental or inadvertent violation.

This is an unintentional, non-habitual violation of privacy that may be caused by lack of knowledge or training, carelessness, or other human error. Examples of this type of incident include:

- Directing confidential information via mail, e-mail, fax, or hand-off to a wrong party, either internal or external to TennCare.
- Leaving confidential information displayed in their workspace such as on computer screens, desktops, or printers where others can view it unnecessarily.
- Repeated Incidental Disclosures.

1.2 Category 2: Failure to follow established security and privacy policies and procedures.

This is a failure to follow appropriate policies with regard to safeguarding confidential information. Examples of this type of incident, include:

- Release of PHI based on invalid member authorization.
- Leaving detailed PHI on an answering machine.
- Failure to report privacy violations.
- Improper disposal of PHI.
- Failure to properly safeguard password.

- Failure to properly conceal or lock a mobile device (i.e. laptop, mobile phone, etc.) used for business purposes, including email, when unattended.
- Transmission of Confidential Information using an unapproved method.
- Leaving Confidential Information unattended in a non-secure area or public area.
- Disclosing enrollee identifiable information by careless telephone use, or discussions in hallways, elevators, the break room, or other work areas.
- Installing devices on TennCare networks that violate TennCare Information Security or Privacy policies, standards, or procedures.
- Download or use of software that has not been approved.
- Repeated instances of behaviors described in Category 1.

1.3 *Category 3: Suspected deliberate or purposeful violation without harmful intent.*

This is an intentional violation due to curiosity, convenience, or desire to gain information for personal use. Examples of this type of incident include:

- Knowingly disabling computer security safeguards without authorization.
- Accessing or attempting to access, or using PHI without a legitimate business need to do so or in violation of applicable policies, standards or procedures. This includes accessing the information of high-profile members, coworkers, friends, family members and others.
- Failure to follow encryption requirements for any device that is used to conduct TennCare business or is used to access TennCare network resources.
- Sharing TennCare system or application credentials (user IDs/passwords) with other workforce member or encouraging others to share.
- Willfully using or disclosing PHI without required authorization.

1.4 *Category 4: Suspected willful and malicious violation with harmful intent.*

This is an intentional violation causing member or organizational harm. Examples of this type of incident include:

- Disclosing PHI to an unauthorized individual or entity for illegal purposes (e.g., identity theft); posting PHI to social media websites; or disclosing PHI to the media.
- Using another employee's password without their knowledge or providing your password to another person associated with harmful intent.
- Unauthorized use or release of data for personal gain.
- Willfully using or disclosing PHI without required authorization.
- Intentionally destroying or altering data in a manner that violates TennCare Records Retention Policies, Standards or Procedures.
- Using or releasing TennCare data with intent to harm or harm the reputation of an individual or the organization.

VI.3 Sanctions/Corrective Action.

The TennCare Privacy Office will work collaboratively with the TennCare Human Resources Department, the

Information Security Office and other TennCare leadership and stakeholders, when applicable, to assure that appropriate and consistent sanctions/corrective actions are applied.

The Privacy Office will issue re-education and privacy awareness training in lieu of referral for formal workforce sanctions at its discretion, in compliance with PRIV-013 Privacy, Security and Confidentiality Training policy. In making this determination, the Privacy Office will consider factors such as violation frequency and severity of violations.

Workforce sanctions shall be administered by the workforce member's supervisory authority and/or the TennCare Human Resources Department and are also subject to the rules of the State of Tennessee Department of Human Resources. Sanctions will be determined on a case-by-case basis and may include discipline, up to and including termination.

The TennCare Privacy and Security Offices recommend the following illustrative sanctions/corrective actions for each category identified above:

1. For privacy violations that fall in Category 1 or 2, as appropriate:
 - Business-Unit lead re-education/retraining of workforce members related to the violation that has occurred.
 - Verbal/Oral Warning related to the violation that has occurred.
2. For privacy violations that fall in Category 3 or 4, as appropriate:
 - Written Warning related to the violation that has occurred.
 - Suspension of AD Accounts.
 - Termination from state employment or removal of vendors and contractor staff from the TennCare project.

There may be situations where AD Accounts or other system access are immediately suspended to remediate an apparent risk of significant compromise to TennCare data or systems. In those situations, immediate action by the Privacy or Security teams shall not constitute formal sanctions. Rather, the formal sanction process will be initiated by Human Resources, if relevant.

For any employee sanctions administered due to incidents involving Federal Tax Information, Human Resources will notify the Chief Privacy and Compliance Officer within 72 hours of initiating a formal employee sanctions process, identifying the individual sanctioned and the reason for the sanction.

OFFICES OF PRIMARY RESPONSIBILITY

TennCare Privacy Office, Office of General Counsel
TennCare Human Resources Department
TennCare Chief Information Security Officer

REFERENCES:

45 C.F.R. § 160.103
45 C.F.R. § 164.501
45 C.F.R. § 164.528
45 C.F.R. § 164.530
T.C.A. § 47-18-2107
T.C.A. § 10-7-307
IRS Pub. 1075
MARS-E 2.2