Division of TennCare

Department of Health Care Finance & Administration
Division of TennCare

Policy Number: PRIV 004	
Policy Subject: Employee Sanctions for Privacy Violations	
Approved by:	**Effective Date: 8/9/2018**

PURPOSE OF POLICY

This policy describes how the Division of TennCare (TennCare) will address privacy violations including unauthorized use or disclosure of enrollee protected health information (PHI) by TennCare workforce members, as regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

POLICY

TennCare will timely respond to all instances of which it becomes aware in which there is unauthorized or inappropriate receipt, use, or disclosure of PHI by an employee or other member of the TennCare workforce. In documented instances of unauthorized access, use, or disclosure of PHI, TennCare will appropriately discipline the employee, up to and including termination from employment. Such sanctions are part of TennCare's compliance with HIPAA and other privacy federal and state laws and regulations.

SCOPE

This policy applies to both TennCare employees and TennCare direct contracted workers who have access to sensitive information such as PHI. This policy's goals may be applied to contract organizations' staff through applicable contractual provisions.

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 Policy, Network Access Rights and Obligation" and "User Agreement Acknowledgement." 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. An example of an incidental disclosure would be an instance in which TennCare employee A is not involved in a particular TennCare service or benefit but inadvertently overhears PHI because of proximity to a conversation TennCare employee B is having regarding that service or benefit. 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.

The result would be different in the above example if employee A re-discloses the PHI in social conversation to TennCare person C or to any person not authorized to have the identifying information. Under those circumstances employee A's re-disclosure would not be an incidental disclosure but would be treated as a violation under this policy.

This policy addresses actions including but not limited to the following:

1) sending an email to the wrong email address or sending without the appropriate level of security;
2) sending one enrollee's PHI to another enrollee, or other releases to persons outside the TennCare workforce or its contracted partners;
3) access by a TennCare workforce member to PHI or other TennCare confidential information for which he or she is not authorized;
4) intentional or reckless distribution of PHI to parties not authorized to have it;
5) sharing of personal network passwords or access codes or documents with other parties that permit them to gain access to enrollee PHI or control of TennCare resources; or
6) knowledge of a violation by another TennCare workforce member occurred and failing to report it.

Both incidental and intentional behavior may be reviewed under this policy; however, intentional misconduct or reckless behavior shall be subject to more significant sanctions.

PROCEDURES:

1. The TennCare Privacy Officer is responsible for receiving, logging, and supervising the investigation of incidents of possible unauthorized uses or disclosures of enrollee PHI. The Privacy Officer will respond to the incident on behalf of TennCare as necessary.

2. If a workforce member believes an inappropriate or unauthorized use or disclosure of an enrollee's PHI has occurred which might not be permitted under HIPAA, such disclosure shall be reported immediately to:

TennCare Privacy Office
Office of General Counsel
310 Great Circle Road
Nashville, TN 37243
Toll-free 1-866-797-9469, Fax (615) 734-5289
Privacy.TennCare@tn.gov

3. Based on departmental policies, the TennCare workforce member disclosing or becoming aware of the authorized use or disclosure should also notify his or her supervisor.

4. TennCare encourages full reporting of disclosures of PHI with the primary focus of mitigation of the harmful effects of any disclosure and review of TennCare processes or employee training which may reduce the likelihood of recurrence.

5. In the event a report of unauthorized disclosure by a TennCare workforce member suggests employee misconduct, the Privacy Officer shall initiate an investigation of the disclosure. She or he may also refer the investigation to the TennCare internal audit or human resources sections, other TennCare departments, or other State agency as appropriate, while maintaining confidentiality during the investigation.

6. All documents and investigation communications shall be treated confidentially as to persons outside TennCare and shall be subject to legal privilege as well as to the provisions of HIPAA. However, in some cases, as per T.C.A. § 47-18-2107, notification of the individual whose personal information was accessed or disclosed shall be required.

7. The TennCare Privacy Officer 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, a division of the Department of Finance and Administration, the Privacy Officer will notify the System Security Officer and/or the TennCare CIO.

8. Upon completion of the investigation, the Privacy Officer will notify the Deputy Commissioner and/or Director of Operations if inappropriate conduct by TennCare personnel is suspected. At that time, the TennCare employee may be referred to the TennCare personnel officer for discipline.

9. Sanctions will be determined on a case-by-case basis, but the following are examples of criteria which might lead to significant discipline, up to and including termination:

a) Any intentional granting of access codes or proxy rights to unauthorized persons which would permit them to have substantial or recurring access to enrollee PHI;
b) Access, use, or disclosure for monetary or other personal gain, with intention to cause harm, disrepute, or otherwise affect a TennCare enrollee or another member of the workforce, or with reckless indifference to TennCare privacy and security policies;
c) Significant harm to TennCare enrollees or to TennCare resources occurring because of or made likely by the employee's action.

10. Any employee sanctions shall be administered by the TennCare Human Resource Department and are also subject to the rules of the State of Tennessee Department of Human Resources.

DEFINITIONS

Encryption: means 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: means an individual applying for or 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 approved pursuant to Sections 1115 or 1915 of the Social Security Act; and, for purposes of the 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: means 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: means 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 employee discuss health information on the phone.

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.

User: means 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.

Workforce: means employees, contract workers, volunteers, trainees, and other persons whose conduct is under the direct control of TennCare.

RELATED FORMS:

Information Loss Worksheet

OFFICES OF PRIMARY RESPONSIBILITY:

TennCare Privacy Office, Office of General Counsel
Chief Information Officer and System Security Officer
Director of Operations and Department of Internal Audit

REFERENCES:

45 CFR § 160.103
45 CFR § 164.501
45 CFR § 164.528
45 CFR § 164.530
T.C.A. § 47-18-2107