



# Bureau of TennCare

## Policy Manual

Policy No: HIP 06-004

Subject: Employee Sanctions for Improper Use or Disclosure of PHI, or for other HIPAA Violations

Approval: *Don J. Gardner by gws*

Date: 9/1/06

### PURPOSE OF POLICY

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

### POLICY

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

### DISCUSSION & LEGAL BASIS

This policy will be interpreted to be consistent with State of Tennessee Security Policies, including but not limited to the Bureau 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.

This Employee Sanctions policy shall include both employees and contract workers who have access to Bureau PHI.

“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 Employee A is not involved in a particular Bureau service or benefit but inadvertently overhears PHI because of proximity to a conversation Employee B is having regarding that service or benefit. The Bureau does not expect such disclosures to be reported if they occur in the normal course of permissible health care operations and the Bureau used means appropriate to the circumstances to limit the disclosures.

The result would be different in the above example, if A re-discloses the PHI in social conversation to Employee C or to any person not authorized to have the identifying information. Under those circumstances A’s re-disclosure would not be an incidental disclosure but would likely be a reportable HIPAA violation under this policy.

This policy on employee sanctions 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 Bureau workforce or its Business Associates;
- 3) access by a Bureau workforce member to PHI or other Bureau 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 Bureau resources;
- 6) knowing of a violation by another Bureau workforce member and failing to report it.

Accidental or 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 the Bureau 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 the TennCare Privacy Officer in the Office of General Counsel. [Privacy.TennCare@state.tn.us](mailto:Privacy.TennCare@state.tn.us) may be used to transmit the report within the State's Groupwise system or other secure (encrypted) means of transmission may be used. One may also call the TennCare Privacy Office or contact the Office of General Counsel (currently 1-866-797-9469 or 615- 507-6830).
3. Depending 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. The Bureau encourages full reporting of disclosures of PHI. The TennCare Privacy Officer shall attempt to mitigate the harmful effects of any inappropriate disclosure and will review office practices or employee training to reduce the likelihood of recurrence.
5. In the event a report of unauthorized disclosure by a Bureau employee or other 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 Bureau internal audit section, other Bureau department, or other State agency as appropriate, being careful to maintain confidentiality during the investigation.
6. All documents and investigation communications shall be treated confidentially as to persons outside of the Bureau and shall be subject to legal privilege as well as to the provisions of HIPAA. However, in some cases, including 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 Draft Policy HIP 06-008. If the release suggests a pattern which may require review or intervention by the Bureau information systems staff or the Office of Information Resources of the Department of Finance and Administration, the Privacy Officer will notify the System Security Officer and/or the Bureau CIO.
8. Upon completion of the investigation, the Privacy Officer will notify the Deputy Commissioner and/or Director of Operations if inappropriate conduct of Bureau personnel is indicated. At that time, the Bureau employee may be referred to the Bureau 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 harm or adversely affect a TennCare enrollee or another member of the workforce, or with reckless indifference to Bureau privacy and security policies;
  - c) Significant harm to TennCare enrollees or to Bureau resources occurring because of or made likely by the employee's action.
  
10. Any employee sanctions shall be administered by the Bureau personnel office and are also subject to the rules of the State of Tennessee Department of Personnel.

## 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). It makes electronic data more secure against viewing in transmission, even if intercepted.

**Enrollee:** means those currently enrolled in all categories 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 the Bureau 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 Bureau operations, such as when a person overhears a nearby Bureau employee discuss health information on the phone.

**Protected Health Information:** (PHI) means medical or health information, including non-medical facts such as address or date of birth, which identify an individual.

**User:** means a member of the Bureau workforce who has responsibility for their individual use of and access to Bureau resources, such as the computer and information the Medicaid management information system.

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

**RELATED FORMS:**

None

**OFFICES OF PRIMARY RESPONSIBILITY:**

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

**REFERENCES:**

45 CFR § 160.103  
45 CFR § 164.501  
45 CFR § 164.528  
45 CFR § 164.530