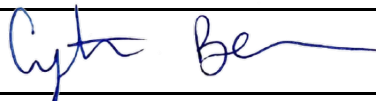


**Department of Finance & Administration
Division of TennCare**

Policy Number: PRIV 001	
Policy Subject: Confidentiality of Enrollee Information	
Approved by: Cynthia Beeler	Effective Date: 07/24/24
Position: Chief Privacy and Compliance Officer	
Signature: 	

I. PURPOSE

The Division of TennCare (TennCare), in conjunction with its Managed Care Organizations (MCOs), Dental Benefits Manager (DBM), Pharmacy Benefits Manager (PBM), and other contractors must ensure that all applicant and enrollee information, materials, and records provided to or obtained by or through said contractors, regardless of medium, will be treated as confidential and as protected health information (PHI) as appropriate.

II. SCOPE

The policy applies to all TennCare employees, consultants, contractors, and other persons who are under the direct or indirect control of TennCare.

III. POLICY

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans and employers. These provisions also address the security and privacy of health data.

In compliance with those provisions, TennCare, MCOs, DBM, PBM and their contracted providers are required to maintain all information about enrollees related to their examination, care, treatment, and payment for such treatment as PHI. This information is not to be released without the enrollee's authorization unless otherwise:

1. required by law;
2. necessary to coordinate the patient's care with physicians, hospitals, or other health care entities;
3. necessary to coordinate insurance or other matters pertaining to payment;
4. necessary in compelling circumstances to protect the health and safety of an individual;
5. necessary for disaster relief or recovery purposes; or
6. necessary for the purpose of health care fraud and abuse detection and compliance; or
7. for purposes permitted under 45 C.F.R. § 164.512.

For all records that TennCare maintains under the Part 2 regulations, TennCare must treat all Part 2 records as confidential and may only utilize them for treatment, payment and healthcare operations purposes as defined by HIPAA if the patient receiving treatment provides adequate consent under Part 2 (PRIV 007 - Information Use and Disclosure Policy). TennCare will follow all regulatory requirements for disclosure of Part 2 information to law enforcement or other legal proceedings, which may require a court order.

Enrollee information *may* be released in response to an order of a court or administrative tribunal and does not require notice to the enrollee, provided that only the PHI expressly authorized by such order is disclosed. Information may be released in response to a subpoena or discovery request in a pending judicial or administrative proceeding not accompanied by a court or administrative order if the enrollee has received actual notice of the request, or if written notice of the request has been sent to the enrollee's last known address.

An enrollee's records may be disclosed, with or without enrollee authorization, to qualified personnel for the purpose of conducting scientific research if approved by an Institutional Review Board (IRB) or a privacy board. Such research may not identify, directly or indirectly, any individual enrollee in any report of the research or otherwise disclose participant identity in any manner. The enrollee's PHI must be adequately stored and processed so that it is protected against unauthorized disclosure (PRIV 018 – Use of Enrollee Records in Research Policy).

TennCare, its MCOs, DBM, PBM, and other contractors must limit the use or disclosure of PHI concerning applicants or enrollees to the minimum necessary to accomplish the intended purpose directly connected with the administration of the plan, except to the extent the use and disclosure is for treatment.

Pursuant to Medicaid confidentiality regulations, TennCare, its MCOs, DBM, PBM, and their contracted providers and subcontracting entities or organizations are required to safeguard information about enrollees. TennCare has data protection standards for public, sensitive and restricted access records outlined in PRIV 027 - Data and Information Systems Classification Policy, and examples of the types of information to be safeguarded are:

1. name, address, and other individually identifiable information;
2. medical services provided;
3. social and economic conditions or circumstances;
4. agency evaluation of personal information;
5. medical data, including diagnosis and past history of disease or disability;
6. information received to verify income or benefits eligibility and amount of medical assistance payments and income information received from the Social Security Administration (SSA) or Internal Revenue Service (IRS); and
7. information received in connection with legally liable third-party resources.

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.

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

Enrollee: An individual applying for or currently enrolled in any of the programs administered by the Division of TennCare, including TennCare Medicaid, CoverKids, Medicare Savings Program, and Long-Term Services and Supports. 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.

Individually Identifiable Health Information: Health information that specifically identifies an enrollee, or there is a reasonable basis to believe that the health information can be used to identify an enrollee.

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.

OFFICES OF PRIMARY RESPONSIBILITY

TennCare Privacy Office, Office of General Counsel (OGC), Managed Care Operations (MCO)

REFERENCES:

42 C.F.R. § 431.300 *et seq.*

42 C.F.R. Part 2

42 C.F.R. § 431.305

45 C.F.R. §§ 160 & 164

45 CFR § 164.502(b)

45 C.F.R. § 164.512

MCO, DBM, and PBM Contractor Risk Agreements

IRS Pub-1075

PRIV- 007 Information Use and Disclosure Policy

PRIV- 018 Use of Enrollee Records in Research Policy

PRIV- 027 Data and Information Systems Classification Policy