STATE OF TENNESSEE

Bureau of TennCare

Acceptable Use Policy: Rules of Behavior

Network Access Rights and Obligations

Purpose

To establish guidelines for access and use of State-owned hardware and software, computer networks and services (such as Internet, email, and telephony), and the security and privacy of users of the State of Tennessee Wide Area Network.

For the purpose of this document, State and TennCare terms shall mean both TennCare's specific resources as well as resources managed on TennCare's behalf by the State of Tennessee. Staff working at or on behalf of TennCare may have access to sensitive personal information such as financial and medical records, income tax data, and social security information. This type of information is subject to stringent controls under federal and state laws and regulations and TennCare policies. These laws and regulations include significant penalties for unauthorized use, disclosure, or exposure of information, both to the agency and to individuals personally.

The primary principle of the TennCare Acceptable Use Policy: Rules of Behavior is:

> *You may use only authorized devices, systems, services and networks when accessing TennCare resources and data; and, you may only perform authorized actions when using TennCare data and resources.*

If you have any question about what resources and services are authorized for your use, ask your supervisor or the TennCare Information Security and Privacy offices.

Objectives

- Ensure the protection of proprietary, personal, privileged, or otherwise confidential data and resources that may be processed in any manner by the State, or any agent of the State.
- Maintain security of and access to networked data and resources on an authorized basis.

- Ensure proper usage of networked information, programs and facilities offered by the State of Tennessee networks.
- Provide uninterrupted network resources to users.
- Protect the confidentiality and integrity of files and programs from unauthorized users.
- Provide Internet and email access to the users of the State of Tennessee networks.
- Secure email from unauthorized access.
- Inform users there is no expectation of privacy in their use of State-owned hardware, software, or computer network access and usage.

Scope

This Acceptable Use Policy applies to all individuals who have access rights through TennCare to the State of Tennessee networks, systems, devices, data, or facilities.

Uses and Prohibitions

Network Resources

TennCare employees and staff from contractors, business partners, and other governmental agencies may be authorized to access state network resources to perform business functions with or on behalf of the State. Users must be acting within the scope of their employment or contractual relationship with the State and must agree to abide by the terms of this agreement as evidenced by his/her signature.

It is recognized that there may be incidental personal use of State Network Resources, however, this practice is not encouraged. Employees should be aware that all usage may be monitored and that there is no right to privacy. Transactions and records resulting from network usage are the property of the State and are thus subject to the Open Records Act.

Prohibitions

- Sending or sharing with unauthorized persons any information that is sensitive by law, rule, or regulation.
- Unsanctioned use or sharing of any TennCare information for personal or financial gain.
- Installing software that has not been authorized by TennCare or the Strategic Technology Solutions division of the Department of Finance and Administration.
- Attaching processing devices that have not been authorized by TennCare or the Strategic Technology Solutions division of the Department of Finance and Administration.

- Using network resources to play or download games, music, or videos that are not in support of business functions.
- Leaving workstation unattended without engaging password protection for the keyboard or workstation.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using network resources in support of unlawful activities as defined by federal, state, and local law.
- Utilizing network resources for activities that violate conduct policies established by the Department of or the Agency where the user is employed or under contract.

Email

Email and calendar functions are provided to expedite and improve communications among network users in order to facilitate official State business.

Prohibitions

- Sending unsolicited junk email or chain letters (e.g. "spam") to any users of the network.
- Sending any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs.
- Sending copyrighted materials via email that is either not within the fair use guidelines or without prior permission from the author or publisher.
- Sending or receiving communications that violate conduct policies established by the Department of Human Resources or the Agency where the user is employed or under contract.
- Sending sensitive material to an unauthorized recipient or sending sensitive email without the proper security standards (including encryption if necessary) being met.

Access to personal email must be from a personally-owned device over a non-State network.

Email created, sent, or received in conjunction with the transaction of official business may be public records in accordance with T.C.A. 10-7-301, and the rules of the Public Records Commission. A public record is defined as follows:

> *"Public record(s)" or "state record(s)" means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency. (T.C.A. 10-7-301 (6)).*

State records are open to public inspection unless they are protected by State or Federal law, rule, or regulation. Because a court could interpret State records to include draft letters, working drafts of reports, and what may be intended as casual comments, be aware that anything sent as electronic mail may be made available to the public.

Internet Access

Internet access is provided to network users to assist them in performing the duties and responsibilities associated with their positions.

Prohibitions

- Using the Internet to access non-State provided web email services. Prohibited access includes reading, or sending email(s), or uploading or downloading attachments.
- Using Instant Messaging or Internet Relay Chat (IRC), or messaging services other than those provided by the State.
- Using the Internet for broadcast audio for non-business use.
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
- Using the Internet when it violates any federal, state or local law.

Working with Confidential Information

Employees at TennCare often work with sensitive information. It is critical that all employees maintain the confidentiality of *all* information. There may be serious consequences to the State, TennCare, and you if any of this information is seen by unauthorized parties. These include disciplinary actions, sanctions, fines or other penalties.

Of note, there are three main categories of confidential information within TennCare:

- Personally Identifiable Information (PII)
- IRS Federal Tax Information (FTI)
- Social Security Administration (SSA) information

Personally Identifiable Information (PII)

PII is defined as any information maintained by an agency about an individual that can be used to distinguish or trace an individual's identity, including:

- Name, social security number, date and place of birth, mother's maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- You may also encounter Protected Health Information (PHI), which is a subset of PII and which is also considered sensitive information that should be treated as such.

- Protected Health Information is defined by HIPAA at 45 CFR 160.103 as 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, employer, or health care clearinghouse; and (2) Relates to the past, present, or future 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.
- PHI includes information that is (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.

IRS Federal Tax Information (FTI)

FTI consists of information sourced directly from the IRS (typically tax return information). Information that is derived or validated against FTI may also fall under FTI guidelines. It is not possible to tell if data is FTI by just looking at it; the root source of the data must be identified to determine if data is actually FTI.

Social Security Administration (SSA) information

Individuals may come into contact with Social Security Administration (SSA) information in the course of their job duties. This information must be treated as sensitive personally identifiable information.

Protecting Sensitive Information

Individuals must be careful to protect sensitive information from being viewed by unauthorized parties. When working with sensitive information on media, such as disks and paper, you are responsible for securely handling this information and must be especially careful that no-one else can access it. Take steps such as:

- Use of removable media, to store sensitive information, is strongly discouraged. In the event it is required, prior authorization must be granted by the employee's supervisor. The privacy and security offices can also provide advice on properly storing and transporting sensitive information.
- Use only media provided and authorized by the State. Do not use personally-owned media.
- Do not use TennCare- or State-provided portable storage devices, such as flash drives or portable disk drives, on external and non-TennCare systems. This is prohibited.
- Do not leave sensitive media unattended, out on a desk or in any other place where someone else might see it.
- Use a secure printer to print sensitive materials. Security PIN should be used for pickup on shared printers.
- Secure paper, disks, thumb drives, and other media in a locked metal cabinet, or other appropriate method.

- If media containing sensitive data must be physically transported, it must be properly encrypted and the Privacy Office informed prior to transportation.
- Do not retain media containing sensitive information any longer than necessary. Destroy the media as soon as it is no longer needed in accordance with all retention, destruction, and litigation hold policies.
- Dispose of paper and recordable discs containing sensitive information in the locked disposal bin designated for sensitive information.

Non-Disclosure

You may only access, use, and discuss records you are authorized to work with and that are necessary for conducting the business tasks assigned to you. You may divulge or discuss sensitive information with TennCare staff or TennCare partners only if you are authorized to do so, and only for legitimate business purposes. Do not access confidential information beyond what is necessary to accomplish assigned work duties.

Accessing, or attempting to access, sensitive information outside of your job duties, or divulging such information to unauthorized parties is grounds for disciplinary action up to and including termination, and/or civil and criminal penalties.

If you are a contractor or work for a third-party provider, your employer is also liable for penalties or sanctions. Your access to and usage of confidential information is logged and monitored, and the logs are reviewed by management.

If you become aware of a data breach or unauthorized release of sensitive information, you must inform the TennCare Information Security and Privacy offices and your supervisor.

If you have any questions about working with confidential data, ask your supervisor and/or TennCare Information Security and Privacy offices.

Alternative Workplace Solutions (AWS) or Equivalent Remote Access

"AWS arrangements utilize mobile technologies, flexible work schedules, and multi-user workstations to maximize efficiency of work processes while reducing costs associated with office space."[1]

The most up-to-date AWS information, policies, and forms can be found at http://hcfaintranet.tenncare.tn.gov/hcfa-library/entry/alternative-workplace-solutions

[1] From the State of Tennessee Alternative Workplace Solutions Policy, http://hcfaintranet.tenncare.tn.gov/assets/docs/uploads/kb/AWSDOHRPolicy.pdf

AWS arrangements include:

- Work from home
- Mobile work
- Free address

State staff authorized to use AWS solutions are responsible for understanding and implementing the policies found in the statewide and TennCare AWS policies and related documents. Your supervisor will work with you to ensure appropriate training and understanding prior to beginning work in this manner.

Staff working remotely will be outside the confines of State-controlled buildings and computer networks. As much TennCare work involves working with sensitive data, such as PII and medical records, every TennCare employee has a special obligation to protect such data from unauthorized disclosure.

AWS Requirements

You *and* your supervisor must:

- Read the complete DOHR AWS policy 14-001, available on the TennCare intranet.
- Discuss all topics on the AWS Employee/Supervisor Discussion Guide; and
- Read and understand the AWS Participation Agreement Form and agree to comply by signing the agreement. A detailed library of statewide, TennCare AWS policies, and other documents is available on the TennCare intranet.
- Use common-sense precautions to protect State- or company-owned device(s) from theft, damage or misuse.
- Do not leave a device unattended in the open: at a coffee shop, in a car, etc. Always keep it under personal control or in a safe place.
- Use a locking cable when a laptop is unattended.
- Always lock the screen when you leave a device unattended, even for a few minutes.
- Use a privacy screen protector when accessing sensitive information in a public place.

Home Devices

Do not use home computers, laptops, tablets, phones, or any other devices not owned, managed, or specifically authorized by TennCare or STS to access, display, store, or process TennCare data. When working with TennCare data from home or other remote sites, you may use only devices and services provided by the State or your employer (if you work for a contracting company). Safety and Security of personal infrastructure is

the responsibility of the individual and shall be considered a public access point for state equipment. Staff will use the provided secure VPN connection at all times when not connected directly to the State network.

Cloud Services

A cloud service is a type of Internet-based computing that provides shared computer storage, processing resources, and data to computers and other devices on demand.

Well-known examples of cloud storage are Dropbox, iCloud, and Google Drive, but there are many others. Use could constitute a security and privacy breach under multiple federal agencies when sensitive data is involved. Do not assume that because a feature or integration is available, such as on a state iPhone, it is approved for use with sensitive data.

Only authorized TennCare resources may be used to conduct TennCare business. TennCare prohibits staff from using unauthorized cloud services for storing or processing TennCare data. In the case where TennCare has approved certain cloud services, TennCare will provide appropriate training and documentation to employees.

If there is any doubt about what resources and services are authorized, contact your supervisor.

Social Media

Social media is a term for internet services that allow information, news, and other content to be shared with others in a social networking context. Common examples of social media include Facebook, Twitter, Instagram, YouTube, LinkedIn, etc.

The State of Tennessee Department of Human Resources (DOHR) addresses the topic in policy *12-058 Personal Use of Social Media*, available on the TennCare intranet.

In addition, there are guidelines on using social media on the State's Portal Advisory Committee web page.

- Personal use of social media on business systems is prohibited.
- Do not act or appear to act on social media for the State of Tennessee or any of its agencies unless expressly approved to do so by the State.
- State employees or contractors cannot use personal social media sites for political purposes, to conduct private commercial transactions, or to engage in private business activities during business hours and with State-issued property.
- State employees are prohibited from using social media to violate any applicable state, federal, or local laws, policies and regulations.
- Posting of sensitive information to social media, networking, or other public website

is strictly prohibited.

Security Handbook

TennCare publishes a security handbook on the TennCare Intranet that all staff must read and remain up to date. It contains definitions of public records; general codes of conduct; best practices; guidelines; whom it applies to; consequences of violating policies; incident response; and, other important security information in further detail.

http://hcfaintranet.tenncare.tn.gov/assets/docs/uploads/kb/securityhandbook.pdf

Incident Response

TennCare publishes a training and quick reference guide for the Reporting of Security and Privacy Incidents that all staff must read to ensure they are aware of the current procedure. This is a one-page guide with instructions in case you witness a suspicious event that must immediately be reported. Please review this guide as part of the acknowledgement of this AUP.

http://hcfaintranet.tenncare.tn.gov/assets/docs/uploads/kb/EndUserIncidentResponseQuickReferenceGuide.pdf

Conflict of Interest

A conflict of interest may occur for the following groups and relationships:

- Family Members: individuals are considered to be a "family member" under the following situations: 1) persons with whom you share a close familial relationship (i.e. your child, grandchild, parent, grandparent, brother/sister, aunt/uncle, niece/nephew or cousin); and 2) relationships by marriage including spouses' immediate relatives to the second degree and the relatives' spouses.
- Close Personal Relationships: these include but are not limited to the following: 1) dating or relationship of co-habitation; 2) domestic partnership; 3) business associates with whom regular business transactions are conducted; and 4) personal friends, i.e. an individual with whom you maintain regular social contact.
  Social Media Relationships: these include individuals with whom you correspond (including, but not limited to, private messages, comments, and posts) on a regular basis through any social media, blog, electronic messaging application, or otherwise.

If you are in a position to access, view, and/or consider client/member data for any purpose, you agree to immediately notify your TennCare supervisor or liaison for reporting to Member Services upon recognizing a connection as follows:

- If you or your family members are enrolled in a TennCare administered program at the time you begin employment.
- When you your family member or someone with whom you maintain a close

personal relationship applies for eligibility of any program administered by TennCare.

- When you, your family member or someone with whom you maintain a close personal relationship files an appeal of any action related to a TennCare administered program.
- When someone with whom you maintain a social media relationship has applied for benefits or is appealing an adverse action.

The following is strictly prohibited:

.

- Accessing TennCare records related to the employee and/or the employee's family members.
- Requesting or influencing a TennCare employee or contractor to access records related to the employee and/or employee's family members.

References

Tennessee Code Annotated, Section 4-3-5501, *et seq.*

Tennessee Code Annotated, Section 10-7-512.

Tennessee Code Annotated, Section 10-7-504.

State of Tennessee Information Security Policies (https://www.teamtn.gov/content/dam/teamtn/sts/sts-documents/Enterprise-Information-Security-Policies-v2-3-ISO-27002-12-21-2018-Inter....pdf)

Section 6.3, Media Handling

Section 9, Mobile Devices and Teleworking.

State of Tennessee Department of Human Resources (DOHR) has a policy *12-058 Personal Use of Social Media* (https://www.teamtn.gov/content/dam/teamtn/agriculture/agriculture-documents/human-resources/12-058%20Personal%20Use%20of%20Social%20Media.pdf)

DOHR AWS policy 14-001 https://www.teamtn.gov/content/dam/teamtn/aws/aws-documents/AWSPOLICYFINAL.pdf

TennCare Incident Response guide for End Users (http://hcfaintranet.tenncare.tn.gov/assets/docs/uploads/kb/EndUserIncidentResponseQuickReferenceGuide.pdf)

You may externally download a zip file containing references in this policy at: https://icaresecureinternal.id.tenncare.tn.gov/documents/34973/3968774/AUP_References.zip

Statement of Enforcement

Noncompliance with this policy may result in the following immediate actions.

- Written notification will be sent to designated TennCare managers and points of contact in the user agency's human resources and Information Technology Resource Offices to identify the user and the nature of the noncompliance as "cause". In the case of a vendor, sub-recipient, or contractor, the contract administrator will be notified.
- User access may be terminated immediately by the Chief Security Officer or Systems Administrator. The user may be subject to subsequent review and action as determined by the agency, department, board, or commission leadership, or contract administrator.

Statement of Consequences

Noncompliance with this policy may constitute a legal risk to the State, an organizational risk to the State in terms of potential harm to employees or citizen security, or a security risk to the State's Network Operations and the user community, and/or a potential personal liability. The presence of unauthorized data in the State network could lead to liability on the part of the State as well as the individuals responsible for obtaining it.

Privacy Expectations

The State actively monitors network services and resources, including, but not limited to, real time monitoring. These communications are considered to be State property and may be examined by management for any reason including, but not limited to, security and/or employee conduct. Users should have no expectation of privacy.

Acknowledgement

As a user of State of Tennessee data and resources under TennCare, I agree to abide by the Acceptable Use Policy and the following promises and guidelines as they relate to the policy established:

- I will protect State sensitive data, facilities, and systems against unauthorized disclosure and/or use.
- I will maintain all computer access codes in the strictest of confidence; immediately change them if I suspect their secrecy has been compromised, and, will report activity that is contrary to the provisions of this agreement to my supervisor or a State-authorized Security Administrator.
- I will be accountable for all transactions performed using my computer access codes.
- I will not disclose any sensitive information other than to persons authorized to access such information as identified by my supervisor.

- I agree to report any suspicious network activity, security breach, or privacy breach per TennCare and State guidelines.
- I will maintain current account and contact information with TennCare's Access Security Team.

I acknowledge that I must adhere to this policy as a condition for receiving access to State of Tennessee data and resources.

I acknowledge that I have read the Computer Crimes Act and TennCare Security Handbook. The locations of TennCare and State of Tennessee's Security policies have been made available. I understand the willful violation or disregard of any of these guidelines, statute or policies may result in my loss of access and disciplinary action, up to and including termination of my employment, termination of my business relationship with the State of Tennessee, and any other appropriate legal action, including possible prosecution under the provisions of the Computer Crimes Act as cited at TCA 39-14-601 et seq., and other applicable laws.

I have read and agree to comply with the policy set forth herein.

Signature: _____

Print Name: _____

Title: _____

Date: _____

TennCare User ID (if provided): _____

TennCare Division
or Company Name: _____

_____

Create Verification PIN (4 digit): _____

If an Organization or Trading Partner account:

I further agree that as a designated representative for the Organization, all documentation is being adequately maintained for all individuals accessing TennCare Systems demonstrating awareness of this Acceptable Use Policy.

Tax ID: _____