



# State of Tennessee Direct Secure Messaging Policies

Version 1.3

## Version History

Version Number	Date	Editor	Remarks
<b>0.0</b>	March 15, 2013	Eric Harkness	
<b>0.1</b>	June 25, 2013	Nathalie Hartert	Removed Process sections
<b>0.2</b>	July 12, 2013	Nathalie Hartert	Merged 2 Policy documents; added forms to Policy Document
<b>0.3</b>	July 22, 2013	Nathalie Hartert Angie Williams	Incorporated team feedback Added Training Section
<b>0.4</b>	July 29, 2013	Sandra Braber Grove, Anne Lovell, Angie Williams, Ricky Tyler, Nathalie Hartert	Included team feedback, updated Breach section
<b>0.5</b>	August 5, 2013	Anne Lovell, Angie Williams, Ricky Tyler, Nathalie Hartert	Included team feedback
<b>0.6</b>	August 19, 2013	Sandra Braber Grove, Anne Lovell, Angie Williams, Regina Nelson Tracy, Ricky Tyler, Nathalie Hartert	Included team feedback
<b>0.7</b>	August 26, 2013	Ricky Tyler Anne Lovell, Lovel VanArsdale, Nathalie Hartert	Updated Access Section, Added Ricky's section about Email Confidentiality, Added Anne's section about Data Use and Handling
<b>0.8</b>	August 27, 2013	Sandra Braber Grove, Anne Lovell, Lovel VanArsdale, Ricky Tyler, Nathalie Hartert	Included team feedback
<b>0.9</b>	August 30, 2013	Sandra Braber Grove, Anne Lovell, Lovel VanArsdale, Ricky Tyler, Nathalie Hartert	Included team feedback
<b>1.0</b>	September 3, 2013	Sandra Braber Grove, Anne Lovell, Lovel VanArsdale, Ricky	Included comments from Sandy, Anne and Angie.

		Tyler, Nathalie Hartert, Angie Williams	
<b>1.1</b>	September 17, 2013	Sandra Braber Grove, Anne Lovell, Regina Nelson Tracy, Lovel VanArsdale, Ricky Tyler, Nathalie Hartert, Angie Williams	Incorporate feedback from State HISP Steering Committee and Tennessee Department of Health attorneys
<b>1.2</b>	September 23, 2013	Sandra Braber Grove, Anne Lovell, Regina Nelson Tracy, Lovel VanArsdale, Ricky Tyler, Nathalie Hartert, Angie Williams	Incorporate feedback from State HISP Steering Committee and Tennessee Department of Health attorneys
<b>1.3</b>	October 7, 2013		Direct Secure Messaging Policies and Forms approved by HCFA Deputy Commissioner

# TABLE OF CONTENTS

INTRODUCTION.....	5
Scope.....	5
Authority and Guidelines.....	5
Complying with the Direct Secure Messaging Policies .....	5
Process for Amending the Direct Policies .....	6
DEFINITIONS .....	7
POLICIES .....	10
1. AUTHORIZATION .....	10
Purpose .....	10
Policies .....	10
2. IDENTITY VERIFICATION / AUTHENTICATION .....	11
Purpose .....	11
Policies.....	11
3. ACCESS, TERMINATION OF ACCESS AND DE-PROVISIONING.....	11
Purpose .....	11
Policies.....	11
4. BREACH .....	13
Purpose .....	13
Policy.....	13
5. SANCTIONS (DISCIPLINARY ACTION) .....	14
Purpose .....	14
Policies.....	14
6. DATA USE AND HANDLING.....	15
Purpose .....	15
Policies.....	15
7. TRAINING .....	16
Purpose .....	16
Policies.....	16
FORMS .....	17

# INTRODUCTION

To the State of Tennessee's Direct Secure Messaging Policies  
For Tennessee State Agencies  
(Hereinafter Participating State Agencies)  
And Authorized Users

## Scope

The scope of these State of Tennessee Direct Secure Messaging Policies ("Direct Policies") includes the full range of privacy and security policies necessary to maintain the confidentiality of Patient Data being exchanged through the Direct Messaging System ("System"), including but not limited to: authorization, identity verification, access, and breach. The State of Tennessee by and through the Department of Finance and Administration (F&A), Division of Healthcare Finance and Administration (HCFA), Office of eHealth Initiatives (OeHI) has developed these Direct Secure Health Messaging Policies. These policies apply to all Authorized Users as defined in the "Definitions Section".

## Authority and Guidelines

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR Parts 160, 162, and 164)
- The Health Information Technology for Economic and Clinical Health Act (HITECH)
- American Recovery and Reinvestment Act (ARRA) of 2009
- Executive Order 35-An order establishing the Governor's eHealth Advisory Council (Governor Bredesen April 6, 2006)
- State HISP Vendor's Certificate Practice Statement (CPS)
- State HISP Vendor's Certificate Policy (CP)
- Implementation Guidelines for State Health Information Exchange (HIE) Grantees on DIRECT Infrastructure & Security/Trust Measures for Interoperability (Office of the National Coordinator – ONC).

## Complying with the Direct Secure Messaging Policies

Each Participating State Agency that has signed an Inter-Agency Agreement and Acknowledgement (Inter-Agency Agreement) between HCFA and the Participating State Agency and wishes to use the State Health Information Service Provider (HISP) services in the State of Tennessee must comply with these Direct Policies.

A Participating State Agency's failure to comply with the Direct Policies stated below constitutes a breach of the Agreement and may result in termination of the Agreement, denial of access to the State HISP Services, or other sanctions as may be designated in the Agreement and in these Direct Policies.

Each Authorized User of a Participating State Agency who has signed an Authorized User Agreement and wishes to use the State HISP Services must comply with the provisions of the Direct Policies that are applicable to Authorized Users.

An Authorized User's failure to comply with the provisions of these Direct Policies applicable to Authorized Users constitutes a breach of the Authorized User Agreement and may result in

termination of the Authorized User Agreement, denial of access to the System by the Authorized User, or other sanctions as may be designated in the Authorized User Agreement and in these Direct Policies.

It is the State of Tennessee's policy to receive Direct messages only from HISPs that are currently accredited by DirectTrust. If a HISP not accredited by DirectTrust wishes to exchange information with the State HISP, the State HISP Governance Committee shall review the facts and issue a decision. If the decision is to permit the non-accredited HISP to exchange information with the State HISP, an agreement shall be entered into between the State, the State HISP Vendor, and the non-accredited HISP.

### **Process for Amending the Direct Policies**

The implementation of any new Direct Policies or the amendment, repeal or replacement of any existing Direct Policies, may occur at any time by notifying all Participating State Agencies at least thirty (30) days prior to the effective date of the change. Within fifteen (15) days of receiving notice of the change, a Participating State Agency may request a delay in the implementation of the change based on unforeseen complications or other good cause. A response to a request to delay implementation will be made within seven (7) days of receiving the request.

## DEFINITIONS

1. **Authorized User** - those persons and non-person entities that have been authorized by a Participating State Agency to send and receive Patient Data through the Tennessee Direct Secure Messaging System (the System). "Authorized Users" may include, but are not limited to, health care providers and employees, staff, contractors, or agents of the Participating State Agency. The Participating State Agency is legally responsible for the actions of each of its Authorized Users with respect to access to the System.
2. **Authorized Agency Representative** - the person who has signing authority on behalf of the Participating State Agency and who signs the "Inter-Agency Agreement and Acknowledgement" form.
3. **Breach of the Security** – federal law defines this as the unauthorized acquisition, including, but not limited to access, use or disclosure, modification or destruction of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by or on behalf of HCFA. Good faith acquisition of personal information by an employee or agent of the information holder is not a breach of the security of the system provided that the personal information is not used or subject to further unauthorized disclosure.
4. **Business Associate** - any person and/or entity that is a business associate of a Participating State Agency under 45 CFR § 160.103.
5. **BYOD** – Bring Your Own Device.
6. **Certificate Authority (CA)** – a trusted organization that maintains and issues digital certificates.
7. **Delegation** – see "Shared Address".
8. **De-provisioning** – the removal of an Authorized User's account from the System.
9. **Direct Account** - the unique identifier for a user or non-person entity to access one or more Direct Mailboxes.
10. **Direct Account Administrator** - the person who manages the Direct accounts for a Participating State Agency. The Direct Account Administrator provisions and de-provisions Direct accounts.
11. **Direct Address** - a Direct-prescribed address identifying both the domain and endpoint within the domain as defined by the Direct addressing specification (E.g. [FirstName.LastName@direct.tn.gov](mailto:FirstName.LastName@direct.tn.gov) or [workerscomp@direct.tn.gov](mailto:workerscomp@direct.tn.gov)).
12. **Direct Credentials** - the combination of the Authorized User's unique identifier (State Network ID, previously known as RACF ID) and Unique Password for a user or non-person entity to access one or more Direct Mailboxes.
13. **Direct Approval Manager** - the person who approves the user to use Direct for sending and receiving Patient Data.
14. **Direct Mailbox** - a computer file or set of files for the collection and storage of email associated with a Direct Address.
15. **Directory** – see "State HISP Directory".
16. **Direct Policies** - the State of Tennessee's written policies pertaining to the use of Direct Secure Messaging and the State HISP.

17. **Direct Security Manager** - the person who verifies the identity of the each Authorized User and each Direct Account Administrator.
18. **Documentation** - all materials, documents, technical manuals, operator and user manuals, flow diagrams, file descriptions, and other written information made generally available by OeHI to users of the System, including all updates thereto, that describe the functions, operational characteristics, and specifications and use of the System.
19. **Effective Date** - the date the Inter-Agency Agreement was signed by Participating State Agency.
20. **HIPAA** - the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by HITECH and as otherwise amended.
21. **HIPAA Regulations** - the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (45 CFR Parts 160, 162 and 164) promulgated by the U.S. Department of Health and Human Services under HIPAA, and as amended.
22. **HISP** - a “Health Information Service Provider”. The HISP processes Direct compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital certificate. Acting in the capacity of an Agent for the State of Tennessee, the HISP holds and manages Public Key Infrastructure (PKI) private keys associated with a Direct digital certificate on behalf of the State of Tennessee.
23. **HITECH** - the Health Information Technology for Economic and Clinical Health Act of 2009 (which is part of the American Recovery and Reinvestment Act of 2009 (ARRA), and as amended including any of the implementing regulations.
24. **Inter-Agency Agreement and Acknowledgement** – the Tennessee State HISP Access Rights and Obligations or Inter-Agency Agreement and Acknowledgement between HCFA and the Participating State Agency.
25. **Local Registration Authority (LRA)** - the Participating State agencies that take on delegated Registration Authority responsibilities for their Direct users and non-person entities.
26. **Log-in Credentials** – see “Direct Credentials”.
27. **MDM** – the State’s Mobile Device Management solution.
28. **Non-person Entity** - a system or application that is authorized by the Participating State Agency to electronically receive or send Direct Messages. (e.g., the Immunization Registry).
29. **Participating State Agency** - a State Agency that is a healthcare provider that transmits any health information in electronic form in connection with a transaction covered by 45 CFR Parts 160, 162, and 164, or a health plan as that term is defined at 45 CFR Part 160.103, in connection with its functions or activities to which this Agreement applies. Each Participating State Agency (i) has been accepted for participation, and (ii) is a signatory to the “Inter-Agency Agreement and Acknowledgement” form.
30. **Patient Data** - all data requested, disclosed, stored on, made available on, or sent by a Participating State Agency, through the System. “Patient Data” includes (i) Protected Health Information; (ii) patient information locator data comprised of domain location, date, type of medical service, class of medical services, Uniform Resource Locator (URL) associated with location of information derived from the patient information made available by a Participating State Agency; (iii) patient demographic data and organization

domain information that is derived from the patient information made available by a Participating State Agency; and (iv) clinical data, medical records, registration information and such other information as shall be consistent with the Direct Policies and made available by a Participating State Agency in accordance with this Agreement.

31. **Protected Health Information or (PHI)** as defined under 45 CFR 160.103 is health information, including demographic information collected from an individual, maintained or transmitted by a covered entity and: (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 information or billing records pertaining to the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
32. **Proxy Access** – see “Shared Address”.
33. **Registration Authority (RA)** - an entity that operates an identity management system (idMs) and collects and verifies Subscriber information on the CA’s behalf. RAs collect and verify identity information from Direct subscribers using procedures that implement identity validation policies.
34. **Shared Access** – shared Access is when an Authorized User delegates access to another Direct mailbox. In the Direct system, an Authorized User will use the Shared Address Management feature to request access to an existing Direct Inbox address. The system receives the request and places the request in the pending approval queue for the Authorized User who is the Owner of the Direct Address for which Shared Access was requested. The system also sends an email to the Authorized User (Owner) mailbox.
35. **State HISP Directory** – the listing of all Authorized Users with a Direct account.
36. **State HISP Governance Committee** – the committee with a representative from each Participating State Agency. The members of the State HISP Governance Committee are security and compliance officers from each Participating State Agency.
37. **State HISP Software** - any software provided in or as an element of the System for the Participating State Agency’s use of the System, including any upgrades of or modifications to such software, or new versions of such software.
38. **State Network ID** – individual user’s logon identification previously known as RACF ID.
39. **State HISP Vendor** - the entity that the State is contracting with to provide the State with HISP, Certificate Authority and Registration Authority services.
40. **Suspension of Access** – the Authorized User’s account has been marked as inactive.
41. **System** - the State HISP portal and Direct Services provided by the State HISP vendor, including the State HISP vendor’s Software and Documentation, for exchange of health information pursuant to this Agreement.
42. **Termination of Access** – suspension or revocation of an Authorized User’s account.
43. **Unauthorized Users** - individuals who accessed the System without the use of authorized credentials or accessed the System by use of a wrongfully obtained password, identifier or log-on.

# POLICIES

## 1. AUTHORIZATION

Authorization is the process of determining whether an individual within a Participating State Agency has the right to access Patient Data via the System. Authorization is based on role-based access standards that consider an individual's job function and the information needed to successfully carry out a role within the Participating State Agency.

### Purpose

To limit the exchange of information to the minimum necessary for accomplishing the intended purpose of the exchange, thereby protecting the privacy of the Patient Data as it moves among Participating State Agencies.

### Policies

#### 1.1. Role-Based Access.

- 1.1.1 Each Participating State Agency shall establish and implement policies that:
  - a. Define what job roles can have a Direct account;
  - b. Define the purposes for which Authorized Users in those roles may access Patient Data via the System, consistent with the limitations set forth in the Participating State Agency Acknowledgement; and
  - c. Ensure that (a.) and (b.) relate to the Authorized User's job function and relationship to the patient.

#### 1.2. Provisioning Direct Accounts.

Each Participating State Agency should leverage existing workflows, policies, and procedures for determining each Authorized User's proxy access to a Direct Mailbox. An Authorized User can have access to multiple Direct Mailboxes, which may be individual and/or role-based.

Each Participating State Agency shall apply the following criteria in provisioning a Direct account to each Authorized User and non-person entities:

- 1.2.1. Authorized Users
  - a. The Authorized User's job description and responsibilities include handling, receiving, and/or transmitting Patient Data, and
  - b. The Authorized User has a @tn.gov domain email address (example: [State.Employee@tn.gov](mailto:State.Employee@tn.gov) or [State.Contractor@tn.gov](mailto:State.Contractor@tn.gov)).
- 1.2.2. Non-Person Entities
  - a. The system or application handles, receives, and/or transmits Patient Data.

#### 1.3. Naming Conventions for Mailboxes

Each Participating State Agency shall examine their current work flows for sending and receiving Patient Data to determine what naming conventions are most appropriate. Depending on business needs and practices, each Participating State Agency may have a mix of individual (e.g., [firstname.lastname@direct.tn.gov](mailto:firstname.lastname@direct.tn.gov)) and role-based Direct Mailboxes (e.g., [cmo.health@direct.tn.gov](mailto:cmo.health@direct.tn.gov); [workerscomp@direct.tn.gov](mailto:workerscomp@direct.tn.gov))

## **2. IDENTITY VERIFICATION / AUTHENTICATION**

Identity Verification, sometimes referred to as authentication, is the process of verifying that an Authorized User seeking to access information via the System is who he or she claims to be and represents an important technical security safeguard for protecting a patient's information from various internal and external risks, including unauthorized access.

### **Purpose**

To verify the identity of the individual who has access to the System.

### **Policies**

#### **2.1. Identity Verification of Authorized Users Prior to Access**

Each Participating State Agency's Security Manager shall verify the identity of each Participating State Agency's Authorized User in accordance with established procedures (refer to the Direct Secure Messaging Procedures and Best Practices Handbook). Each Participating State Agency may delegate this responsibility to a Registered Sub-Organization (e.g. A County Health Department) and the Sub-Organization's Security Manager.

## **3. ACCESS, TERMINATION OF ACCESS AND DE-PROVISIONING**

Access controls govern when and how a patient's information may be accessed and/or exchanged by Authorized Users.

### **Purpose**

To minimize unauthorized access and ensure that Patient Data is only used for authorized purposes by ensuring that: (1) only Authorized Users access information via the System; and (2) Authorized Users do so only in accordance with the requirements (specified herein) that limit their access to specified information (e.g., that which is relevant to a patient's treatment).

### **Policies**

#### **3.1. General**

Each Participating State Agency shall enter into an Inter-Agency Agreement and Acknowledgement between HCFA and the Participating State Agency prior to being granted access to and use of the System.

#### **3.2. Granting Access to Authorized Users**

Each Participating State Agency shall be responsible for facilitating each Authorized User's access to the System. Each Participating State Agency is legally responsible for the actions of each of its Authorized Users with respect to access to and use of the System.

- 3.2.1 Each Participating State Agency shall identify individuals within its organization who need access to the System to carry out their professional responsibilities. These may include, but are not limited to, healthcare providers, employees, staff, contractors, or agents of Participating State Agency.
- 3.2.2 Each Participating State Agency shall identify a Direct Security Manager who is responsible for verifying the identity of each Authorized User. The Direct Security Manager shall do so in accordance with these established policies and the procedures contained in the Direct Secure Messaging Procedures and Best Practices Handbook.
- 3.2.3 Each Participating State Agency shall identify a Direct Account Administrator who is responsible for granting access to each Authorized User, including requiring that each Authorized User signs an Authorized User Agreement and takes the steps necessary to obtain a user name and password. Authorized Users shall be informed of who serves as the Direct Account Administrator within the Participating State Agency for all questions, training, and to whom reports of any potential unauthorized access shall be made. This contact information shall be readily available to each Authorized User within the Participating State Agency.

### **3.3. Access Specifications**

Each Authorized User shall select his/her State Network ID (RACF ID) as the unique User ID. Each Authorized User shall select a unique password, in accordance with the State of Tennessee's Enterprise Information Security Policies to access Patient Data via the System.

- 3.3.1 Each Authorized User shall be authenticated in accordance with the policies in Section 2 of this document.
- 3.3.2 Temporary user names shall be prohibited.
- 3.3.3 Each Authorized User shall not share his or her Log-In Credentials with others and shall not use the Log-In Credentials of others. See Sanctions Section.

### **3.4. Authorized Purposes**

Each Participating State Agency shall permit each Authorized User to access and exchange Patient Data via the System only for purposes consistent with the Inter-Agency Agreement, these Direct Policies, and the Authorized User Agreement.

### **3.5. Confirmation of User Population**

Semi-annually, OeHI shall send a list of Authorized Users to each Direct Account Administrator within each Participating State Agency. Each Participating State Agency shall confirm each Authorized User's continued need for a Direct account.

### **3.6. Password management**

Each Authorized User shall follow the State of Tennessee's Enterprise Information Security Policies regarding password management available on the OIR Intranet at <http://intranet.tn.gov/finance/oir/security/policy>.

### **3.7 Termination of Access**

Each Participating State Agency shall develop procedures to terminate the access of an Authorized User, including the suspension of the account prior to termination. Access to the System shall be suspended or terminated:

- a. Immediately following a reported or suspected breach by an Authorized User;
- b. Immediately upon notification of termination of an Authorized User's employment or affiliation with the Participating State Agency;
- c. Immediately following a change in job responsibilities of the Authorized User such that access to the System is no longer needed;
- d. At the Participating State Agency's discretion, when an Authorized User is out on extended leave;
- e. Immediately upon suspicion of compromised Authorized User account; or
- f. Upon the willful violation or disregard of any of these policies.

### **3.8 De-provisioning**

Each Participating State Agency or the Direct Account Administrator in the Participating State Agency shall, in accordance with the procedures set forth in the State HISP Procedures and Best Practices Handbook, de-provision an Authorized User's account when the Direct Approval Manager approves such action.

### **3.9 Termination/De-provisioning Notification**

Each Participating State Agency or the Direct Account Administrator in the Participating State Agency shall, in accordance with the procedures set forth in the State HISP Procedures and Best Practices Handbook, inform the OeHI if at any point an Authorized User's access has been suspended, terminated, or de-provisioned. The OeHI shall then inform the State HISP provider.

## **4. BREACH**

The State HISP is committed to protecting the privacy, security and confidentiality of the data being accessed and exchanged via the System at all times including if and when a breach occurs.

### **Purpose**

To report, investigate and mitigate any harm that a breach or suspected breach may cause.

### **Policy**

#### **4.1 Incident Response Plan**

Each Participating State Agency shall develop an Incident Response Plan (IRP). The IRP shall provide that, in the event the Participating State Agency becomes aware of any suspected or actual Breach of the Security of Unsecured Patient Data, the Participating State Agency must assess the probability that the Patient

Data has been compromised based on a risk assessment that considers at least the following factors:

- a. The nature and extent of the Patient Data involved, including the types of identifiers and the likelihood of re-identification;
- b. the unauthorized person to whom the disclosure was made;
- c. whether the Patient Data was actually acquired or viewed; and
- d. the extent to which the risk to has been mitigated.

#### **4.2 Breach Notification and Reporting**

- 4.2.1 Each Participating State Agency shall notify HCFA's Privacy Office IMMEDIATELY upon becoming aware of any actual or suspected breach of the security and/or privacy of the data being accessed and exchanged via the System.
- 4.2.2 Initial notification shall be made by telephone or e-mail to HCFA's Privacy Office.
- 4.2.3 Each Participating State Agency shall complete, with as much information as possible, HCFA's "Loss of PHI/PII Worksheet" ([https://tn.gov/assets/entities/tenncare/attachments/phi\\_piiworksheet.pdf](https://tn.gov/assets/entities/tenncare/attachments/phi_piiworksheet.pdf)) within FORTY-EIGHT (48) HOURS of the reported event.

#### **4.3 Breach Investigation**

- 4.3.1 Each Participating State Agency shall conduct an investigation upon the report of an actual or suspected breach of the data accessed or exchanged via the System.
- 4.3.2 Each Participating State Agency shall submit its initial findings of any investigation of an actual or suspected breach of the data accessed or exchanged via the System in an initial Breach Investigation Report to HCFA's Privacy Office within FORTY-EIGHT (48) HOURS of the reported event.
- 4.3.3 Each Participating State Agency shall submit a final Breach Investigation Report to HCFA's Privacy Office within THIRTY (30) CALENDAR DAYS of the reported event.

## **5. SANCTIONS (DISCIPLINARY ACTION)**

### **Purpose**

To inform each Participating State Agency and Authorized Users about possible sanctions for misuse of the System.

### **Policies**

- 5.1 When misuse of the System has occurred, each Participating State Agency may, at its discretion, impose disciplinary action, up to and including requiring the Authorized User to undergo additional training in the use of the System, termination of access, termination of employment, and/or termination of the Inter-Agency Agreement and Acknowledgement between HCFA and the Participating

State Agency and any other appropriate legal action, including possible prosecution under all applicable laws.

## **6. DATA USE AND HANDLING**

Each Authorized User has a responsibility to ensure the protection of Patient Data that is viewed, shared or discussed through Direct Secure Messaging to be consistent with the HIPAA Privacy and Security Rules and HITECH, including prohibiting disclosures to unauthorized individuals.

### **Purpose**

To ensure each Authorized User understands and follows the requirements for the exchange, use and handling of patient data.

### **Policies**

#### **6.1 Personally Owned Devices**

The use of personally owned devices is STRICTLY PROHIBITED.

The use of State owned devices (e.g. smart phones, other mobile and cellular phones and tablets) that are managed by the State's Mobile Device Management (MDM) solution shall be permitted only when used in accordance with the State HISP Procedures and Best Practices Handbook.

#### **6.3. Data Use**

Each Authorized User shall only use the data for the specific reason for which he or she received the data.

#### **6.4. Data Handling**

6.4.1 Each Authorized User shall not make copies of Patient Data unless permitted by the Participating State Agency, the Direct Secure Messaging Policies or applicable law.

6.4.2 Each Authorized User shall not view, save, print, e-mail, download, copy, photograph, or otherwise replicate Patient Data from the System to any personal media or devices.

6.4.3 Each Authorized User shall not view, save, print, e-mail, download, copy, photograph, or otherwise replicate any Patient Data to any un-encrypted state-owned mobile media or mobile devices.

#### **6.5 Disclaimer**

Each Authorized User shall include the following disclaimer in each transmission made using the System: "This message and any attachment to this message are intended solely for the individual or entity to which it is addressed and may contain CONFIDENTIAL and/or PRIVILEGED material. Any review, retransmission, dissemination or other use of or taking action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you have received this email in error please contact the sender and delete the material."

#### **6.6 Recipient and Content Verification**

Each Authorized User shall ensure that the recipient, content and attachment of the message are what they are intended to be **PRIOR** to sending the secure message.

## **6.7 Confidentiality Controls**

Each Authorized User shall adhere to the following confidentiality controls to protect the patient data:

- a. sign out of the System at the end of each session;
- b. lock his or her computer before leaving his or her workstation to prevent others from accessing the System; and
- c. make sure that he or she has signed out of the System at the end of each day.

## **7. TRAINING**

### **Purpose**

To ensure that each Authorized User is trained on the proper use of the System and is made fully aware of the policies and procedures to be adhered to when using the System.

### **Policies**

#### **7.1. Privacy, Security and Confidentiality (PSC) Training**

- 7.1.1 Each Participating State Agency shall annually provide on-site training, web-based training, or comparable training tools to ensure that each Authorized User is familiar with these Direct Policies governing privacy, security and confidentiality when accessing and exchanging information via the System. This training may be provided in conjunction with the Participating State Agency's regular HIPAA/HITECH training activities.
- 7.1.2 Each Participating State Agency shall ensure that each Authorized User signs a Statement of Understanding showing that he or she has received PSC training and has agreed to comply with the Direct Policies and with the Participating State Agency's own privacy and security policies and procedures. Such certification shall be retained by the Participating State Agency for a minimum of six (6) years.

#### **7.2. System Training**

Each Participating State Agency shall ensure that each Authorized User undergo continuing and/or refresher training on a periodic basis as a condition of maintaining authorization to access the System. At a minimum, each Participating State Agency shall provide additional training when the State HISP has been modified and/or updated. This training may be provided in conjunction with the Participating State Agency's PSC training activities.

# FORMS



## STATE OF TENNESSEE

### Tennessee State HISP Access Rights and Obligations

#### Inter-Agency Agreement and Acknowledgement between HCFA and Participating State Agency

Tennessee Direct Secure Health Messaging System (“System”) facilitates the secure electronic exchange of Patient Data through the Tennessee Health Information Service Provider (HISP). Access to the HISP is granted to each State Agency that has entered into an Inter-Agency Agreement and Acknowledgement (“Inter-Agency Agreement”) with the Department of Finance and Administration (F&A), Division of Healthcare Finance and Administration (HCFA). This Agreement is required prior to being granted access to and using the System.

*The Participating State Agency agrees to abide by the following (**Please have the Authorized Agency Representative initial each item**):*

- \_\_\_\_\_ All use of and interactions with the System by Participating State Agency (and its Authorized Users) will be in compliance with the Direct Secure Health Messaging Policies, this Agreement, including all exhibits and applicable federal and State laws and regulations and as amended.
- \_\_\_\_\_ Participating State Agency is responsible for facilitating each Authorized User's access to the system in a manner that allows HCFA to rely on Participating State Agency for authentication and authorization of each Authorized User in accordance with the Direct Secure Health Messaging Policies.
- \_\_\_\_\_ Participating State Agency or the Direct Account Administrator in the Participating State Agency will use the procedures set forth in the State HISP Procedures and Best Practices Handbook, to inform the OeHI if at any point an Authorized User's access has been revoked, suspended, terminated, or de-provisioned. The OeHI shall then inform the State HISP provider.
- \_\_\_\_\_ Participating State Agency will designate individuals to serve in the following roles: Authorized Agency Representative, Direct Approval Manager, Direct Security Manager and Direct Account Administrator.
- \_\_\_\_\_ Participating State Agency will designate a single point of contact to serve as its organizational liaison to HCFA for technical, operational, and clinical issues.
- \_\_\_\_\_ Participating State Agency will maintain, in full working condition, at its own expense, any technical interfaces in its possession, if applicable.

\_\_\_\_\_ Participating State Agency will, upon request, provide HCFA all information regarding results of system testing activities, results of pilot testing, and similar developmental and operational issues.

**Participating State Agency:**

\_\_\_\_\_  
Type or Print Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Authorized Signature

\_\_\_\_\_  
Date

**HCFA:**

\_\_\_\_\_  
Type or Print Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Authorized Signature

\_\_\_\_\_  
Date



# STATE OF TENNESSEE

## Authorized User Identity Verification Form

Instructions for completing the Identity Verification Form by an Authorized User:

1. This form must be completed in its entirety by the Authorized User and reviewed by the Direct Security Manager.
2. The Authorized User **must present in person two types of identification from the list below (one must be a photo ID)** to the Direct Security Manager, as proof of identity. The Direct Security Manager is responsible for validating the Identity of the Authorized User.
3. Once signed by the Authorized User and the Direct Security Manager, the Direct Security Manager retains the Authorized User Identity Verification Form in accordance with State Policy.

The following types of identification may be used, if they are current, i.e. not expired.

- A current document issued by the federal government or a state, county, municipal or other local government and containing the person's photograph, signature and physical description
- A current driver license or current identity card issued by any state
- A current United States passport or a current officially recognized passport of a foreign country. A United States passport means a U.S. passport and a U.S. passport card issued by the U.S. Department of State.
- A current United States military identification card or draft record
- A current identity card issued by a federally recognized Indian tribe
- Voter's Registration card
- Birth Certificate
- US Coast Guard Merchant Mariner Card
- US Citizen ID Card (Form I-197)

To Be Completed By Authorized User

Full First Name and Full Last Name (print)

<b>Title</b>
<b>E-mail Address</b>
<b>Business Phone Number</b>
<b>Department of Health License Number (if applicable)</b>
<b>Participating State Agency Name</b>
<b>Authorized User Signature</b>

To Be Completed By Participating Agency Security Manager	
<p>I hereby certify that on this _____ day of _____, 20_____</p> <p>_____ personally appeared before me, signed or attested in my presence, and presented the following two forms of identification as proof of his/her identity.</p>	
Photo ID	Expires/Issued
And	Expires/Issued
Printed Name of Agency Security Manager	
Direct Security Manager Signature	



# STATE OF TENNESSEE

## Direct Account Administrator Acknowledgement

Tennessee Direct Secure Health Messaging System (“System”) facilitates the secure electronic exchange of Patient Data through the Tennessee Health Information Service Provider (HISP). Access to the HISP is granted to each State Agency that has entered into an Inter-Agency Agreement and Acknowledgement (“Agreement”) with the Department of Finance and Administration (F&A), Division of Healthcare Finance and Administration (HCFA). Your State Agency has designated you as a Direct Account Administrator to manage individual Direct accounts for each Authorized User in your agency. As a Direct Account Administrator you have elevated privileges, greater responsibility and are held to higher standards related to maintaining the confidentiality, security and integrity of Patient Data.

As a Direct Account Administrator for the Tennessee Direct Secure Health Messaging System, **in addition to items agreed to on the Authorized User Acknowledgement Form**, I further agree to abide by the following (please initial each item):

- \_\_\_\_\_ I shall not create an account for an Unauthorized User.
- \_\_\_\_\_ I shall not give additional permissions or privileges to any Authorized User without proper authorization.
- \_\_\_\_\_ I shall be accountable for all transactions performed using my Direct Account Administrator credentials.
- \_\_\_\_\_ I shall report to the Participating State Agency any suspicion or belief that the credentials of any Authorized User have been compromised and shall follow the Participating State Agency’s procedures to mitigate damages.
- \_\_\_\_\_ I shall report to the Participating State Agency any suspicious activity, suspected security breach, or suspected security incident related to the use of the Tennessee Direct Secure Health Messaging System.
- \_\_\_\_\_ I shall report to the Participating State Agency any suspected violation revealed during the review and audit of any Authorized User’s use of the Tennessee Direct Secure Health Messaging System.
- \_\_\_\_\_ I understand the willful violation or disregard of any of these statutes or policies may result in my loss of access to and use of the System, my removal as Direct Account Administrator, 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 Tennessee Personal and Commercial Computer Act as cited at TCA 39-14-601 et seq., and other applicable laws.

\_\_\_\_\_  
Type or Print Name

\_\_\_\_\_  
State Network User ID

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date



# STATE OF TENNESSEE

## Tennessee State HISP Access Rights and Obligations Authorized User Acknowledgement

### Terms of Access to Tennessee State HISP and Direct Secure Health Messaging

Tennessee Direct Secure Health Messaging System (“System”) facilitates the secure electronic exchange of Patient Data through the Tennessee Health Information Service Provider (HISP). Access to the HISP is granted to each State Agency that has entered into an Inter-Agency Agreement and Acknowledgement (“Inter-Agency Agreement”) with the Department of Finance and Administration (F&A), Division of Healthcare Finance and Administration (HCFA). Your State Agency agrees to provide you with access to the HISP only if you agree to comply with the Direct Secure Messaging Policies, which are intended to maintain the confidentiality, security and integrity of Patient Data.

You must agree to abide by the following (please initial each item):

- \_\_\_\_\_ I shall never reveal my Login Credentials to anyone.
- \_\_\_\_\_ I shall not allow others, including other staff members with whom I work, to access the State HISP using my Login Credentials.
- \_\_\_\_\_ I shall log out of the HISP before leaving my workstation to prevent others from accessing the HISP.
- \_\_\_\_\_ I shall not fax/print/email/download/copy/photograph or otherwise provide Patient Data to any third parties except in accordance with the Direct Policies and applicable law.
- \_\_\_\_\_ I shall not make unauthorized copies of the Patient Data.
- \_\_\_\_\_ I shall not save Patient Data to any personal media or devices except in accordance with the Direct Policies.
- \_\_\_\_\_ I shall not save any Patient Data to any un-encrypted state-owned media or devices except in accordance with the Direct Policies.
- \_\_\_\_\_ I shall not access the HISP via public-use workstations or devices. Public-use workstations and devices are those where general public access is allowed.
- \_\_\_\_\_ I shall not use the HISP or access or view any Patient Data except as required for my job.

\_\_\_\_\_ I shall notify my State Agency point of contact immediately upon becoming aware or have reason to believe that my Login Credentials have been compromised.

\_\_\_\_\_ I understand that my State Agency has the right at all times to review and audit my use of the HISP and compliance with the Direct Secure Messaging Policies.

\_\_\_\_\_ I shall maintain the confidentiality of all information in accordance with HIPAA and all other state and federal laws governing the privacy and security of health information, and in accordance with State Agency's privacy and security policies and procedures as well as the Direct Secure Messaging Policies.

\_\_\_\_\_ I understand the willful violation or disregard of any of these statutes or policies may result in my loss of access to and use of the System 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 Tennessee Personal and Commercial Computer Act as cited at TCA 39-14-601 et seq., and other applicable laws.

\_\_\_\_\_  
Type or Print Name

\_\_\_\_\_  
State Network User ID

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date