



**Secure Email Information for Sending and Receiving for both DIDS
Staff and Providers or Other Outside entities.**

Secure Email Overview 2
Secure Email Tracking Possibilities 2
DIDS sending a Secure Mail – how and what happens 3
The Outside State’s Network Server receiving a Secure Mail – how and what happens... 5
The Outside State’s Network User setting up password and password reset questions 7
The Outside State’s Network view of the Secure Email..... 8
The Outside State’s Network Management of Secure Email using the State’s Secure Web
Server 9
Four Day notice to both DIDS staff and the Outside State’s Network Recipient of the
Secure Email 10
Possible Security Alert..... 12
Replying to Secure Mails from outside and inside the State’s Network 12
Password Reset 13
Support and Help 13

Secure Email Overview

Secure Email communication is necessary because of the growing regulatory demands and security concerns. Secure Email is needed for the protection of information that contains HIPAA or other information specific to an individual demographics, services or specific enough to identify that individual. The State of Tennessee has two different conditions in which Secure Email can be processed.

The first is called Gateway to Gateway. This is when the Secure Email is electronically “encrypted” so that only the sending mail server and the receiving mail server are able to view. This is possible only when the State’s Secure Email Server and the Receiving Email Server are able to “exchange” a “security certificate”. In this type of Secure Email, the Receiving Email Entity does not have to do anything. They will not notice any change in the look of mails that they receive.

The second condition in which a Secure Email can be processed by the external receiving entity is to create an account within the State’s network so that they can view the mail. This is required if the receiving individual’s mail server is not able to “exchange” a “security certificate” with the state. In this example, the “mail” never leaves the State’s network so the protection of information is always “inside”. In this condition, the receiver of the Secure Mail will receive an email notifying them that they have received a Secure Mail and a link to log into the States Secure Email Server and view their mail.

NOTE:

In both of these Conditions, The DIDS staff must always create the mail using the same criteria...putting [secure email] in the subject line of the mail. This is required for all mails that need to be secure.

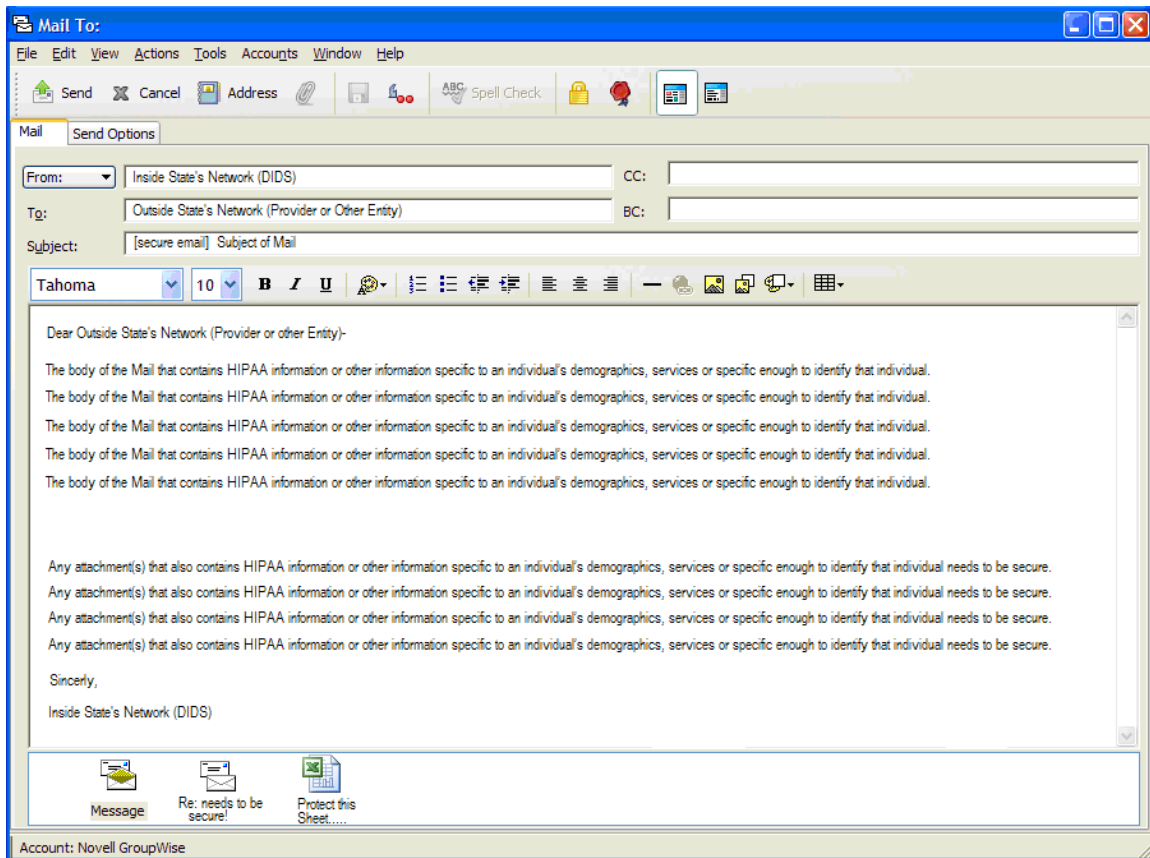
Secure Email Tracking Possibilities

- When “DIDS” sends a Secure Mail out to an “Outside State Network” entity
- When the “Outside State Network” entity replies to a “DIDS” Secure Mail
- When an “Outside State Network” sends a Secure Mail to “DIDS”
- When “DIDS” replies to an “Outside State Network” entity’s secure mail

DIDS sending a Secure Mail – how and what happens

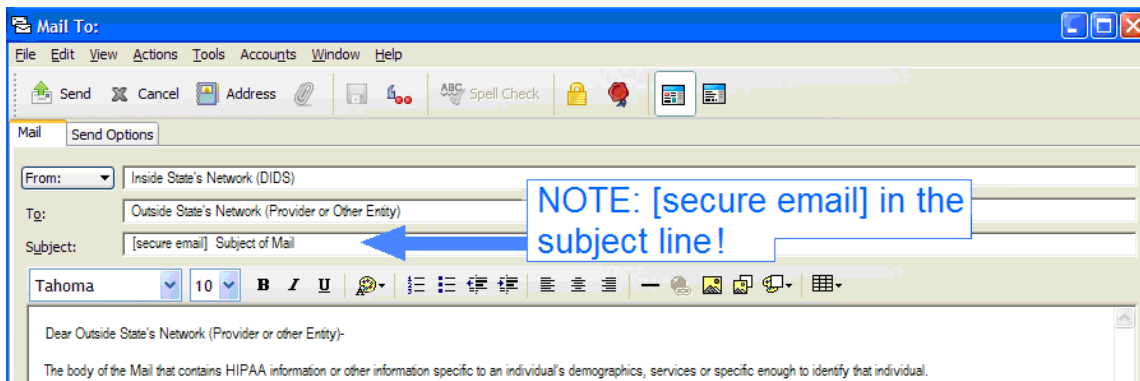
For all DIDS staff who are sending a mail to an outside state network address that contains HIPAA Information or other information specific to an individual's demographics, services or specific enough to identify that individual, the DIDS staff must put [secure email] in the subject line of that mail.

Here is an example of what the DIDS GroupWise mail would look like:



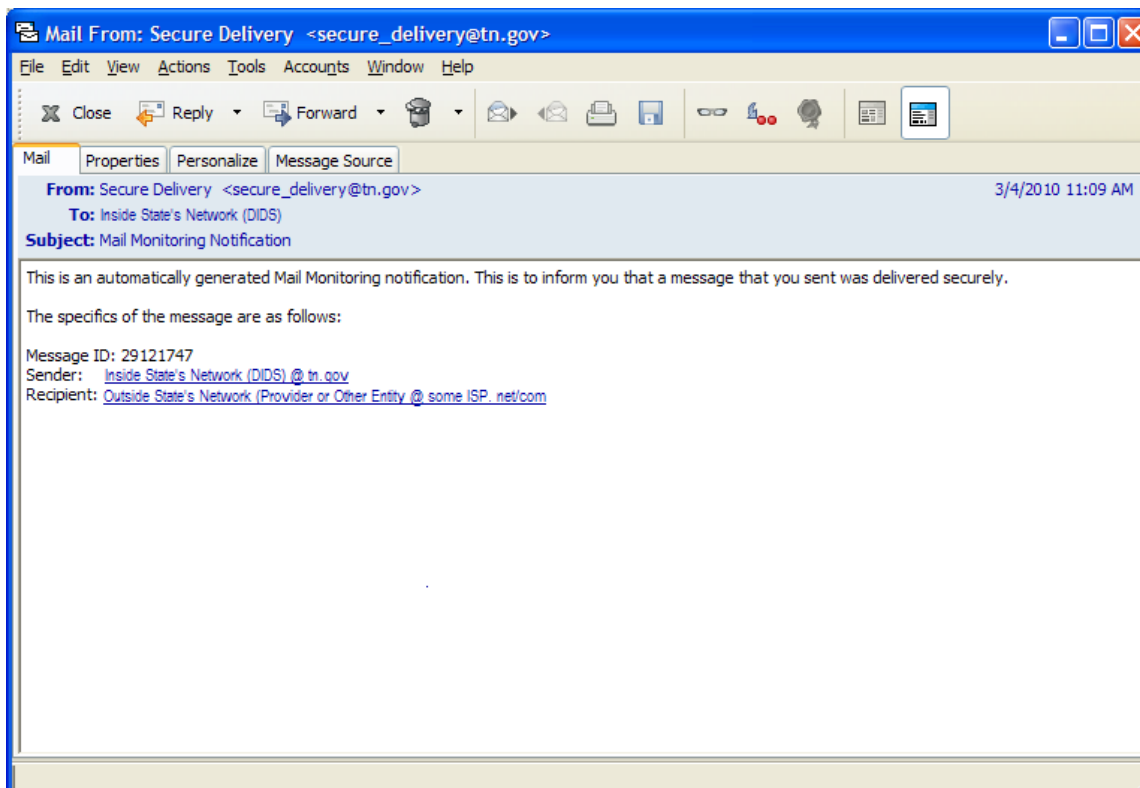
Secure Email Information and Overview

The [secure email] must be put in the subject line for the State's Mail Server to manage appropriately! This is the only way that a mail will be secure protecting HIPAA and other personal information.



Once the Secure Email has been sent, the DIDS staff will receive a confirmation in their GroupWise mail account. This is an auto generated mail sent from the Secure Email Server. If you do not receive this notice, the mail that was sent was not sent "secure".

Here is an example of the notification that the DIDS staff will receive from the State's Secure Email Server:



The Outside State's Network Server receiving a Secure Mail – how and what happens

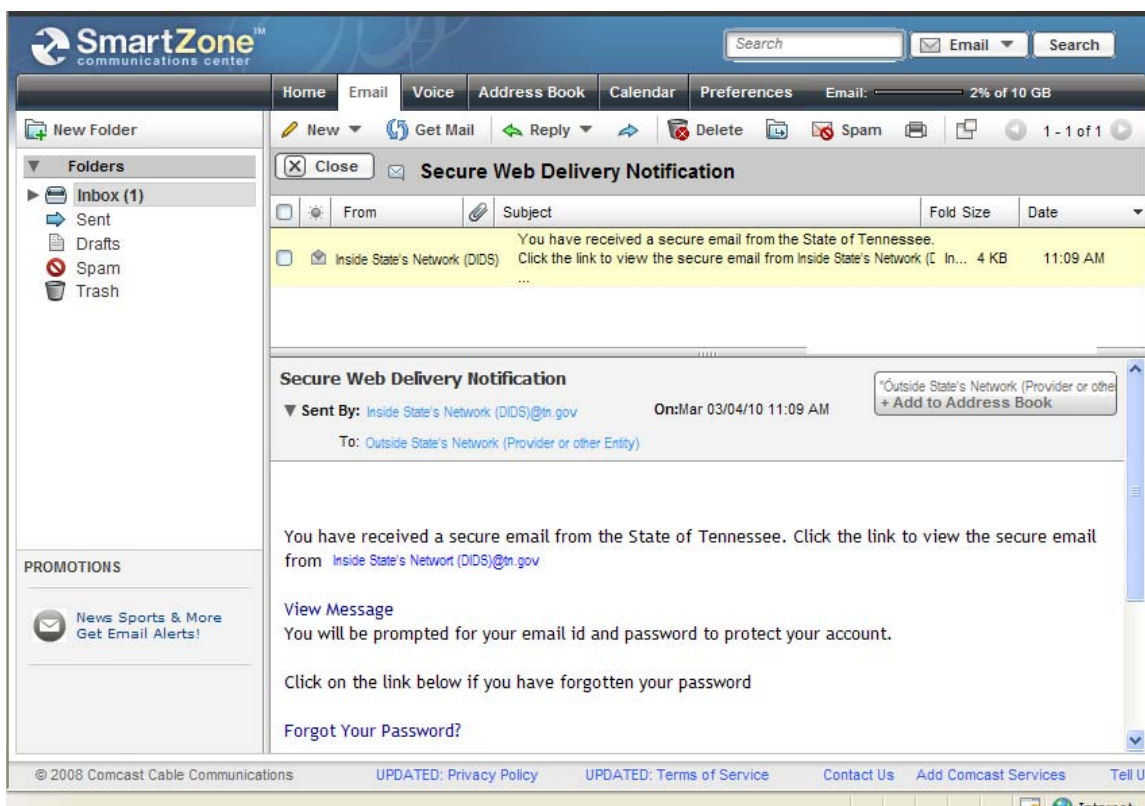
For Providers and other Non State Entities that are receiving a Secure Email from DIDS one of the following two things will occur:

The Outside State's Network receiver will be able to view their mail as always. There are not any other steps that need to be taken. (In this example, the Outside State Mail Server was able to exchange the State's "security certificate" allowing the encrypted mail to be viewed correctly.)

Or

The Outside State's Network receiver will receive a notice telling them that they have a secure email and to view it they need to create an account inside of the State's Secure Mail Server. Once the receiver's email account has been setup, the user will not be forced to do this again.

An example of what this mail looks like is below:



Secure Email Information and Overview

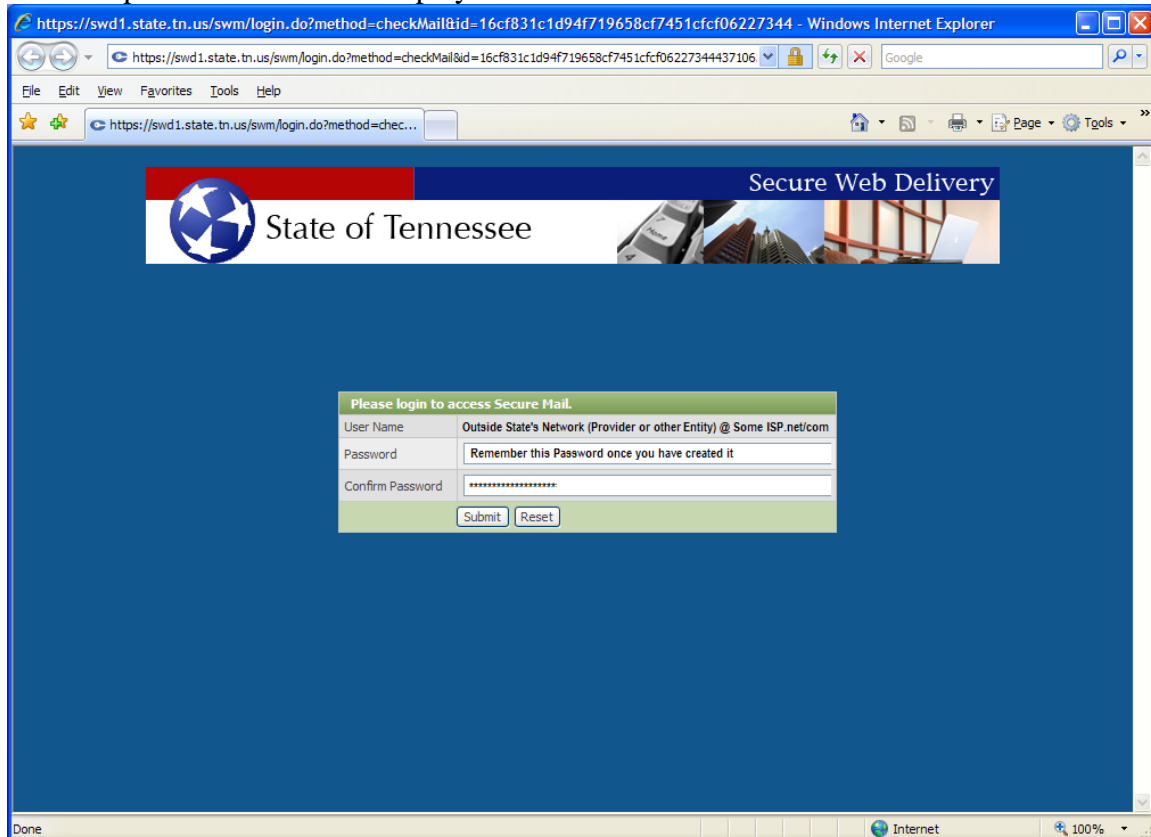
Receivers of a Secure Email need to click on the “View Message” hyper link that will take them to log in screen so that they can create an account with the Secure Email Server or view their mail.

Please see screen shot below:



For Outside State’s Network first time users, the Secure Email Server will force them to create an account on the Secure Web Delivery server inside the state’s network. Users need to “register” the email address that the Secure Mail was sent to. This is the tracking method that the Secure Web Delivery server uses.

An example of this screen is displayed below:

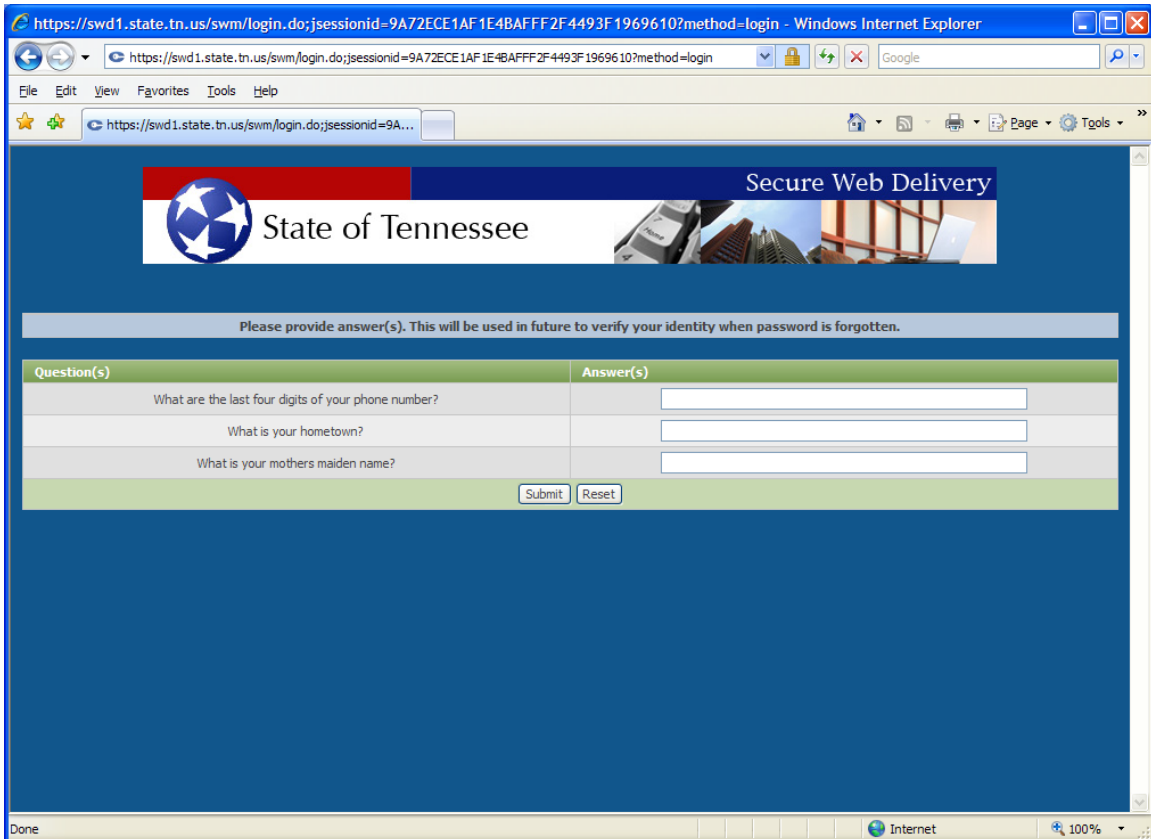


The Outside State's Network User setting up password and password reset questions

The Secure Web Delivery Server will force new users to enter in answers to Security Questions. This is to setup an Automatic Security Password reset option in the event that the Outside State's Network user forgets their password.

The Outside State's network user has to establish their email on the State's network to view any mails sent to that address. They only have to do this one time. However, each time they need to view additional mails that have been sent using the [secure email] format, they will have to log onto that account using their password.

An example of the Security Questions Screen is below:



The screenshot shows a web browser window with the URL <https://swd1.state.tn.us/swm/login.do?jsessionId=9A72ECE1AF1E4BAFFF2F4493F1969610?method=login>. The page header includes the State of Tennessee logo and the text "Secure Web Delivery". Below the header, a message states: "Please provide answer(s). This will be used in future to verify your identity when password is forgotten." The main content area contains a table with two columns: "Question(s)" and "Answer(s)".

Question(s)	Answer(s)
What are the last four digits of your phone number?	<input type="text"/>
What is your hometown?	<input type="text"/>
What is your mothers maiden name?	<input type="text"/>

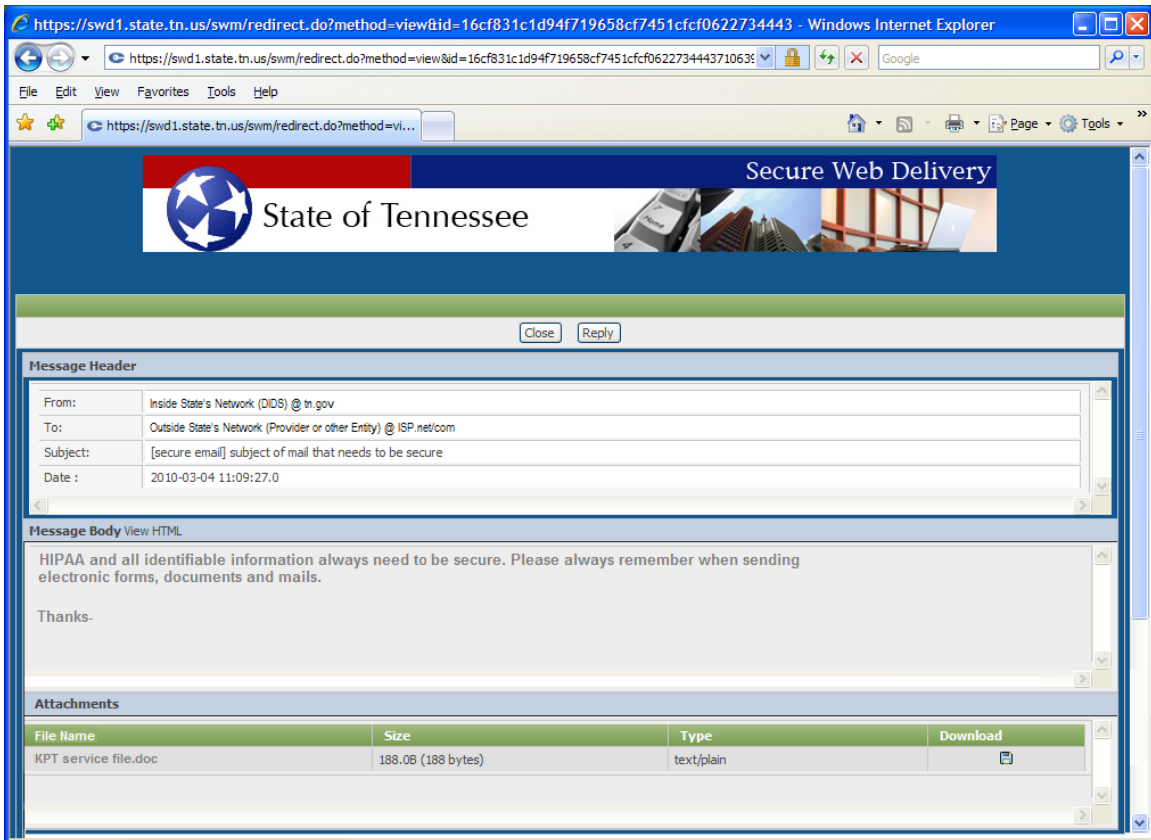
At the bottom of the table are "Submit" and "Reset" buttons.

The Outside State's Network view of the Secure Email

Once the account has been established for the email address on the State's Secure Web Mail Server they will be able to view the secure mail that they have received. Because the user has logged into the State's Secure Web Delivery Server, all parts of the mail are protected. This also includes any attachments that were sent with the mail.

Please note that the user only has a few options in the management of Secure Email that are viewed from the State's Secure Web Delivery Server. The Secure Email recipient can "Read", "Reply To" and "Delete" messages from the secure site. The email recipient cannot "forward" the message or "modify" the text of the original message from the secure website.

An example of this is below:



The Outside State’s Network Management of Secure Email using the State’s Secure Web Server

The management of the Secure Email that a user receives is limited to only two options. The user can double click on a mail to view the message for the first time or reread (there is no limit to the number of times a mail can be viewed in the 14 day period prior to deletion) or they can check the “Delete” box with will allow the Secure Web Server to remove the mail.

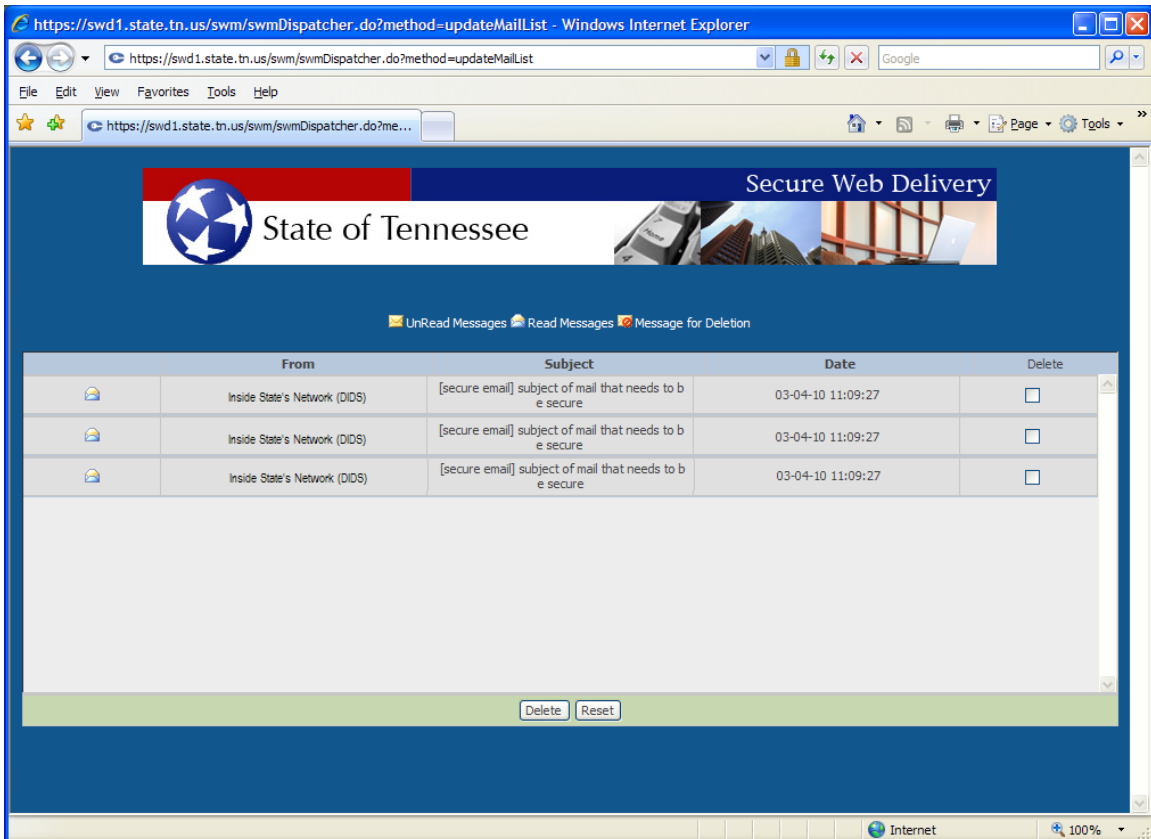
NOTE:

All emails and associated attachments that are sent via the State’s Secure Email Delivery are automatically deleted. The following procedures define this “clean-up” of the Secure Web Server:

- Opened/Viewed - Deleted fourteen (14) calendar days after the message has been opened/viewed by the external recipient
- Un-opened/Not Viewed – deleted fourteen (14) calendar days after the notification message has been delivered to the external recipient.

NOTE: There is no notice on the fourteenth (14) day that the mail will be deleted or has been deleted.

An example of a User’s Secure Management screen is below:

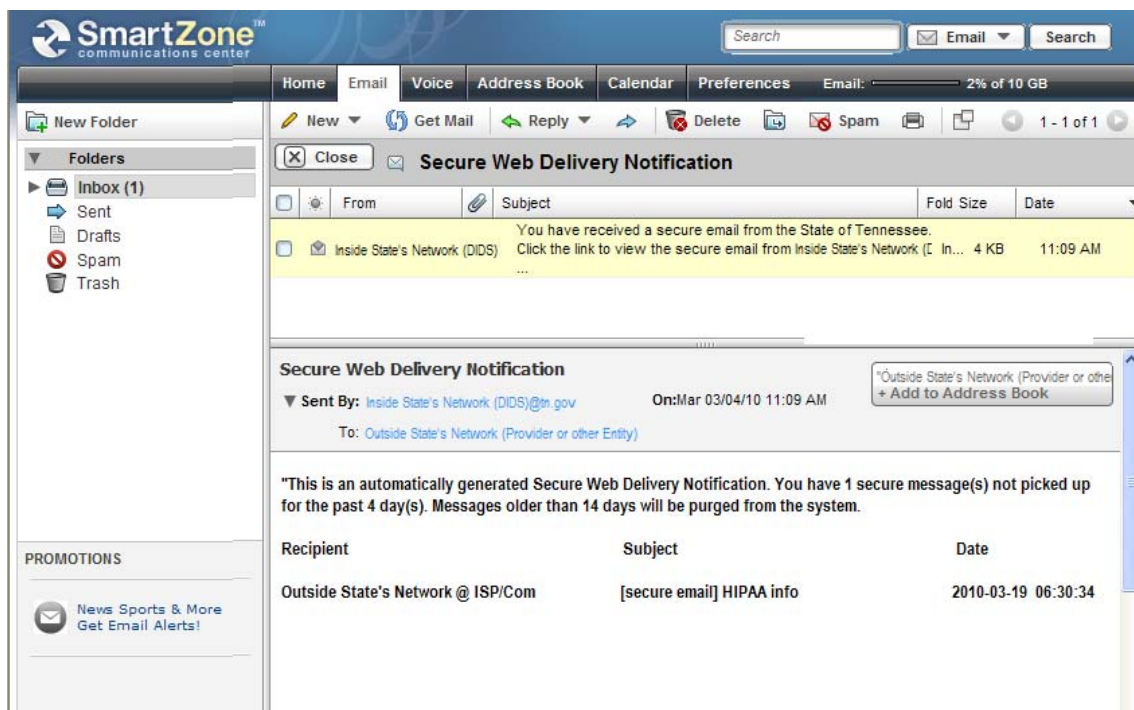


Four Day notice to both DIDS staff and the Outside State's Network Recipient of the Secure Email

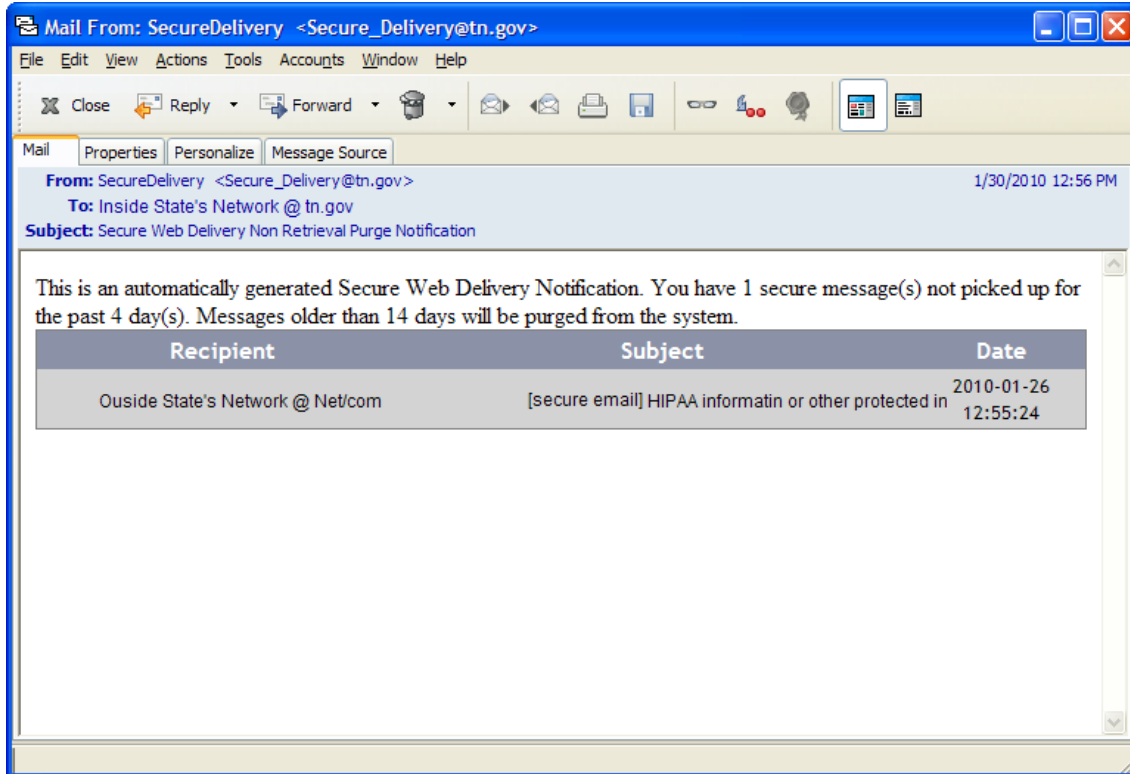
The State's Secure Web Email system will provide a notification to both the sender and all receivers of a [secure email] that has not been opened in four calendar days. This notice will only happen on the fourth day. This notice is only a "tickler" and to inform the DIDS sender that their mail has not been reviewed. There are not any other notices provided by the Secure Web Email Server. On the fourteenth day, the mail and any attachments to the mail will be deleted.

An example of this notification for both the DIDS staff and the Outside State's Network Recipient is below:

To Outside State's Network Recipient Notice



DIDS Staff Notice



Possible Security Alert

Depending on how the Outside State's Network recipient's Internet browser is setup the following message could display. If a user receives this message when attempting to navigate to the Secure Web Email Server they should select "Yes" to proceed.

Below is an example of what this message could look like:



Replying to Secure Mails from outside and inside the State's Network

Users whose Email Servers are able to "exchange" a "security certificate" with the State's Security Email Server can reply to the sender without making any other changes or special procedures. If you are able to receive mails this way, there is no problem with replying to them. The State's Secure Email Server will continue to keep the mail secure.

Users that have to log onto the State's Secure Web Email Server to view their emails can reply to mails using the Secure Web Email. This is one of the options available once the user has logged into the State's Server.

DIDS staff who respond to any mail (one that initiated from an outside entity or one that initiated from inside the state) and that mail needs to be secure, they need to add [secure email] to the subject line.

NOTE:

If the conversation began from the State and [secure email] was already in the subject line, DIDS staff do not need add [secure email] in the subject line again. Examples of this could be:

Re: [secure email] HIPAA information

Fwd: Re: [secure email] HIPAA information

As long as [secure email] in anywhere in the subject line, the State’s Secure Web Server will be able to identify it and protect the contents.

Password Reset

Users from outside the State’s Network who forget their password can have it automatically reset by clicking on the “forget your password” link. This link will direct them to the Security Questions that were setup when the account was created. Once the user answers all the questions correctly and submits the answers, the system will send to the user their new password. After the user logs into the State’s Secure Web Email Server they will be able to reset the password if needed.

An example of the “forget your password” link is below:



Support and Help

DIDS users who need help or support can contact the DIDS Help Desk at:

MRHelpDesk@tn.gov
615-532-9670 -Office
615-532-7552 -Fax

Users from outside the State’s Network need to contact the sender of the secure email for assistance. The DIDS staff that sent the Secure Email will be able to direct non-state users in how to retrieve their mail. If the DIDS staff is unable to resolve the outside user’s

issue, the DIDS staff will initiate a HelpDesk ticket. This allows the Business side to determine if the issue is training or technical.

If it is a technical issue, the DIDS Business Partners will send an email to MRHelpDesk with the provider name, phone number and issue. The IT Team will contact the provider to resolve issue and contact the business partner and let them know the issue is resolved.

When contacting the DIDS HelpDesk, it is important to give them all of the contact information possible. Examples of this are:

- Your RACF ID (for state employees)
- Provider Agency
- Provider Employee Name
- Email Address
- Phone Number