Secure File Delivery Application

Phase 1: Outbound Files from MassHealth

USER GUIDE

www.mass.gov/masshealth

November 2004

DISCLAIMER

PLEASE READ THIS NOTICE CAREFULLY. BY USING THE SECURE FILE DELIVERY APPLICATION, YOU AGREE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SECURE FILE DELIVERY APPLICATION.

The Commonwealth of Massachusetts, Executive Office of Health and Human Services ("MassHealth") is making the Secure File Delivery Application available for use by you and other receivers of MassHealth files "AS IS," without charge. No express or implied warranty is offered by MassHealth. Your use of the Secure File Delivery Application is entirely voluntary. By using the Secure File Delivery Application, you assume sole responsibility for the results of your use, and agree to hold harmless MassHealth, its contractors, including the Unisys Corporation, and its suppliers, including Authentica, Inc., from any claims by you or any third party arising out of your use, even if such claim results from an error or defect in the application.

Much effort has been expended to make the Secure File Delivery Application reliable and easy to use, but it is not guaranteed to be free of error. We invite you to inform us of any defects or errors you discover in the application, but we do not promise that any error or defect can be or will be corrected. In no event shall MassHealth, its contractors, or its suppliers be liable to you or to any third party for any damages of any kind, including without limitation, direct, indirect, special, consequential, or punitive damages arising out of your use of the Secure File Delivery Application.

TABLE OF CONTENTS

Introducing the Secure File Delivery Application 1

Key Features 1

Getting Started with the Secure File Delivery Application 1

Minimum System Requirements 1
How to Register to Use the Secure File Delivery Application 2
How to Retrieve a File from the Secure File Delivery Application 2

Other Secure File Delivery Application Functionality 6

Sent Items Link 6
New Message Link 6
Change Password Link 6
Address Book Link 7
Help Link 7
Log Out Link 7
On Screen Help 7

Troubleshooting Secure File Delivery Application Issues 7

Introducing the Secure File Delivery Application

Welcome to Authenticas Inc.'s Secure File Delivery Application– MassHealth's recommended solution for Trading Partners to receive the 835 (Health Care Claim Payment/Advice transaction), 820 (Payroll Deducted and Other Group Premium Payment for Insurance Products transaction), 834 (Benefit Enrollment and Maintenance transaction), 997 (Functional Acknowledgment transaction), and Supplemental Electronic Proprietary Remittance Advices for non-retail pharmacy providers. The Secure File Delivery Application is a Web application that provides a fast and secure way for you to receive messages and attachments over the Internet. The Secure File Delivery Application Content server works like an e-mail application. However, MassHealth can ensure protection and control of content during delivery.

To open protected files, you will need to log in with your Username and password. Once you log in and authenticate your identity, the protected content opens if you have permission. You can then perform various actions on the content, for example, print, copy and paste. Any access limits depend on the type of protection the sender used and the permissions that the content allows.

Note: *This User Guide only covers functionality present in Phase 1 of the rollout of the Secure File Delivery Application. It does not detail features associated with Phase 2 of this project (files sent from outside entities to MassHealth), such as the "Sent Items", "New Message", and Address Book links. It does not detail how to use the Secure File Email features.*

Key Features

Some of the more prominent features of the Secure File Delivery Application include:

- Quicker receipt of your files
- Email notification that there is a file available to be picked up
- Reduced manual intervention in the delivery process
- All information is encrypted to ensure security & privacy

Getting Started with the Secure File Delivery Application

This section describes the recommended minimum system requirements for the Secure File Delivery Application, how to register for a Username and Password, and how to retrieve a file.

Minimum System Requirements

- Microsoft Internet Explorer version 5.5 or higher browser or a Netscape Navigator version 4.7.9 or 6.2.2.
- Anti-virus software installed on your PC and network.

Note: *In addition, a signed Trading Partner Agreement on file with MassHealth, a valid email address, and a* **Username and Password** *are required to run Secure File. (Refer to the "How to Register to use the Secure File Delivery Application" section of this document to learn how to get a Username and Password.)*

How to Register to Use the Secure File Delivery Application

- Contact the MassHealth HIPAA Support Center at 888-848-5068 or send an e-mail to MAHIPAASUPPORT@unisys.com, and request to be registered to use the Secure File Delivery Application.
- You will need to provide:
  - Your organization's name.
  - Your MassHealth Provider Number.
  - A contact name.
  - A contact number.
- A valid functional email address to which your notification email will be sent. (**Note***:* A functional mailbox is an e-mail address that is not tied to a specific individual. For example, securefile@acmehospital.org is a functional mailbox; b.jones@acmehospital.org is not.)
  - What transaction(s) you would like to receive via the Secure File Delivery Application. Example: 835 & Supplemental Electronic Proprietary Remit.
- You will subsequently receive an e-mail detailing your user name and password.

How to Retrieve a File from the Secure File Delivery Application

1. When MassHealth sends you a file using the Secure File Delivery Application, you will receive a notification email (see example below) that includes a link to the login page of the Secure File Delivery Application.

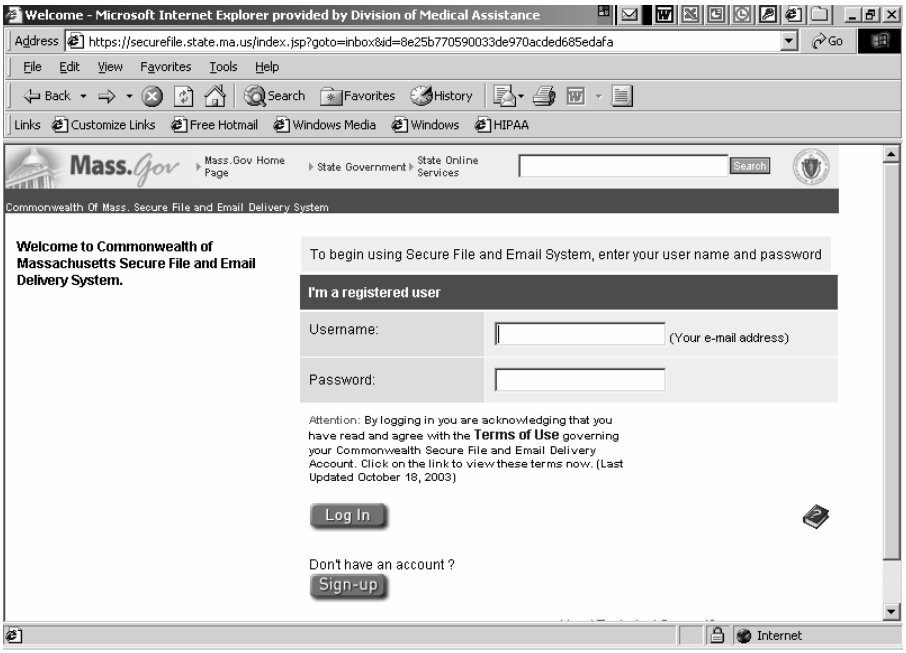
From: MassHealthsecurefile@nt.dma.state.us.com
Sent: Friday, January 16, 2004 8:06 AM
To: Olsen, David (Acme Hospital)
Subject: Commonwealth Of Massachusetts Secure E-Mail RE: Secure File Delivery test message

You have received a message or file containing protected information sent through the Commonwealth of Massachusetts' Secure File Delivery and Email Delivery System. Please enter your Commonwealth Secure File Delivery and Email Delivery System Password and I.D. in order to retrieve this message. Please note that this message has been sent through the Secure File Delivery and Email Delivery System because it is confidential information, improper use or disclosure of which may subject you to civil or criminal fines or imprisonment. Do not use the Password/ID of another person to access the waiting message or messages. They are intended only for the person who owns the email address on this message." Click here to view it. If you do not have a Commonwealth Secure File Delivery and Email Delivery System Password and I.D. please register for one. If you can not see the link, please copy and paste the following URL into your Web browser:

https://securefile.state.ma.us/inbox/get_message.jsp?eid=8e25b770590033de970acded685edafa

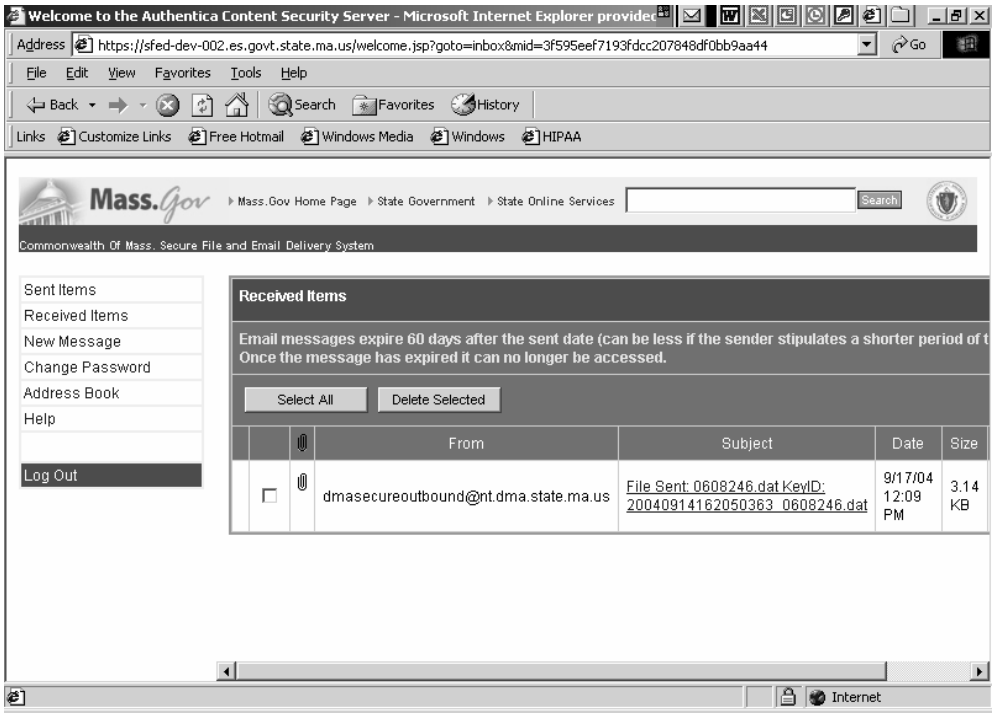
It is suggested that your password be at least 8 characters in length, include upper+lower case characters, and at least one number. Do not pick a password that could be easily guessed by a third party who is familiar with you, such as your street address, or the names and ages of your children.

2. Click on the "Click here" link or, if you can't see the link, copy the URL provided in the notification email into your Web browser. This will bring you to the Secure File login page, which will look as follows:



3. Enter the Username that MassHealth assigned to you in the "Username" field and press Tab on your keyboard.

4. Enter the password that MassHealth assigned to you in the "Password" field and press Enter on your keyboard. This will take you into your Secure File "Received Items" mailbox:



This page appears when you attempt to open a message protected with the Content Security Server or when you first log in to the Content Security Server. It allows you to see a list of all the messages sent to you. You can open them and delete them when necessary.

Note: *You will only be able to access your files for 30 days after receipt of your notification email. Therefore, we strongly recommend that you download your files in a timely matter and save them locally. If you need to access a file after the 30-day expiration interval, please contact the MassHealth HIPAA Support Center at 888-848-5068 or MAHIPAASUPPORT@unisys.com.*

The Received Items page contains details on the e-mail address of the sender, message subject, date and time sent, size of the file, and protection level used (Standard). You can determine if the message contains an attachment since those messages appear with a paperclip icon in the item row. Unread messages appear in bold on this page. The Received Items page contains this information:

Select All/Deselect All- Click the "Select All" button to select all the messages on the Received Items page. A check appears in the box next to each message and the button name changes to "Deselect All". To deselect all the messages, click the button "Deselect All".

Delete Selected- Click this button to delete all the selected messages. (If you ever need to add the message to your list again, click on the link to the protected content from your notification message.) This only removes the message from your Received Items page. Messages will automatically be deleted from the Content Server after 30 days.

From- Lists the e-mail address of user who sent you the message.

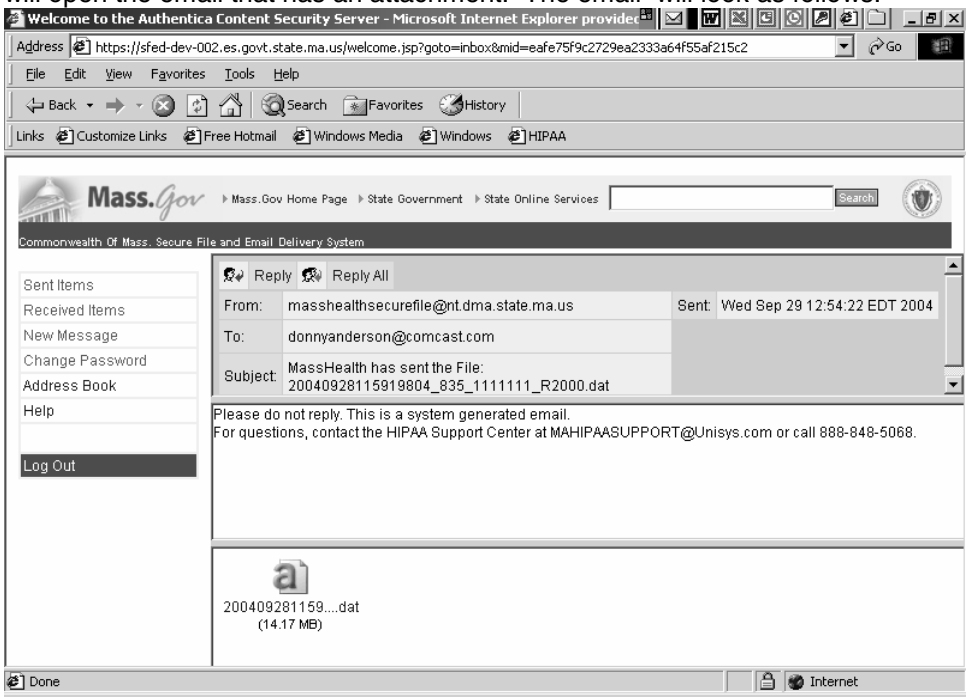
Subject- Lists the subject you used for message. Click on the message subject to open the message.

Date- Lists the date and time you received the message.

Size- Indicates the size of the message.

Protection- Lists the protection level used for the message. The protection that senders can use depends on how their Content Security Server administrator set up their system. The standard level protects the message and any attachments through delivery.

5. To retrieve a file, click on the dynamic link in the “Subject” column for that file. This will open the email that has an attachment. The email will look as follows:



Note: *Please do not use the “Reply” or “Reply All” function, as your email will be sent to a mailbox that is not monitored. Please direct all Secure File Delivery Application emails to the MassHealth HIPAA Support Center at MAHIPAASUPPORT@unisys.com.*

6. To download the file to your PC, right click on the file name and choose “Save Target As…”. Select the folder on your PC where you would like to save this file and click the “Save” button.

7. Secure File Delivery Application File Name Changes

The files sent to external entities by MassHealth via the Secure File Delivery Application will be data files (they will have a .dat file extension). MassHealth will also be adding a unique prefix [MassHealth’s Secure File Database Timestamp (expressed in CCYYMMDDHHSSSS)_File Type_ Provider #] to each Secure file for audit purposes. As a result, the file naming convention for the 820, 834, 835, 997, and Supplemental Electronic Proprietary Remittance Advice will be different when it is sent via the Secure File Delivery Application. The table below details examples of how the file is currently named vs. how it will be named for the Secure File Delivery Application.

Transaction	Current File Name	Secure File Name
835	1000100_R1790.835	2004100119423814_835_100100_R1790.dat
820	1000100_820M_11.820	2004100119423218_820_1000100_820M.11.dat
834	834D_31.dat	2004100119423502_834_1000100_834D_31.dat
997	1000100.997	2004100119424005_997_100100.dat
Electronic Remit	1000100_R1790_INV09.txt	2004100119424258_EMC_100100_R1790_INV09.dat

Other Secure File Delivery Application Functionality

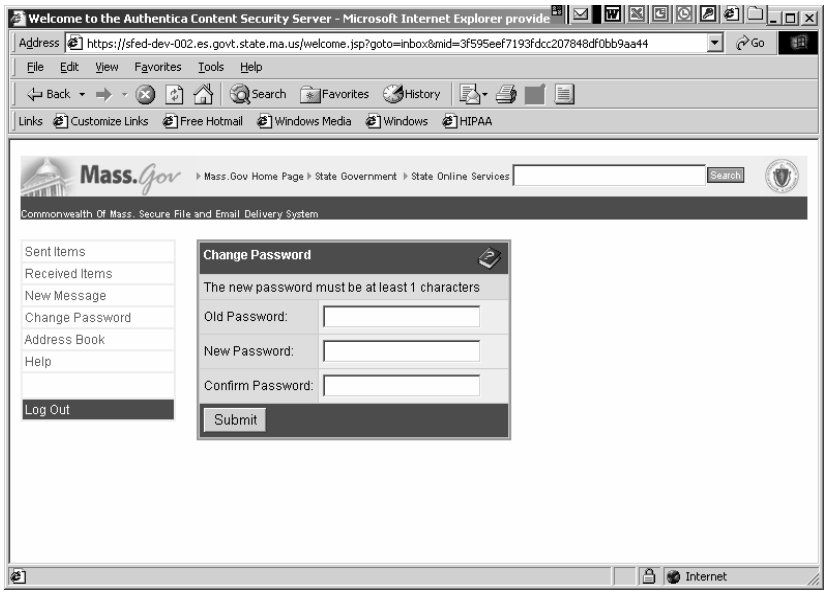
Sent Items Link

Please do not use. This functionality will not be available until Phase 2 of this project. (**Note**: If you are an MCO copay file submitter, you may already have this functionality).

New Message Link

Please do not use. This functionality will not be available until Phase 2 of this project. (**Note**: If you are an MCO copay file submitter, you may already have this functionality).

Change Password Link



This page appears after you log in to the Content Security Server Web application and click Change Password or when you forget your password and go through the process of resetting it by clicking the “Forgot your password?” link on the Welcome Page. You cannot reset your password if you did not register for your user name and password the first time you logged in to the Content Security Server. You may want to change your password periodically to ensure better security. If this page appears after you click the “Forgot your password?” link, it has the following fields:

Password- Enter a new password (8 alphanumeric characters with at least 1 uppercase letter, 1 lowercase letter, and 1 number).

Confirm- Enter your password again to confirm it.

If this page appears after you log in to the Content Security Server Web application and click Change Password, it has the following fields:

Old Password- Enter your current password.

New Password- Enter a new password (alpha or numeric characters).

Confirm Password- Enter your password again to confirm it.

Address Book Link

Please do not use. This functionality will not be relevant until Phase 2 of this project. (**Note**: If you are an MCO copay file submitter, you may already be using this functionality).

Help Link

The help link provides an overview of the Secure File and Email Delivery Application.

Log Out Link

Click on this link to log out of the Secure File Delivery Application.

On Screen Help

After you log into the Secure File Delivery Application, just click on the Help icon on any page to get related help information.

Troubleshooting Secure File Delivery Application Issues

Contact the MassHealth HIPAA Support Center at 1-888-848-5068 or MAHIPAASUPPORT@unisys.com. The MassHealth HIPAA Support Center will contact you once a resolution is reached.