

**MICHIGAN DEPARTMENT OF
COMMUNITY HEALTH**

**DRAFT
ELECTRONIC SUBMISSION
MANUAL**

June 1, 2013

Submitting
Electronic Health Care Transactions

Table of Contents

Section 1 - INTRODUCTION	4
Section 2 - RESOURCES	5
Section 3 - SOFTWARE AND PROGRAMMING	6
Section 4 - DATA EXCHANGE GATEWAY (DEG).....	7
4.1 DEG - DIAL-UP CONNECTION	7
4.1.1 Hardware, Software and Connection Requirements.....	7
4.1.2 Dial-Up Specifications	7
4.1.3 Setting up the MDCH Dial-Up Connection.....	8
4.1.4 Logging onto the MDCH Dial-Up Connection	15
4.1.5 FTP Specifications	16
4.1.6 FTP Commands	17
4.2 DEG - INTERNET CONNECTION.....	18
4.2.1 PC Setup	18
4.2.2 Logging onto the MDCH Internet Connection	19
4.2.3 Downloading Files from the DEG.....	20
4.2.4 Uploading Files to the DEG	22
Section 5 - SSLFTP/SFTP (WS_FTP) SETUP FOR THE DEG.....	24
5.1 Overview	24
5.2 WS_FTP Pro Version 2007.....	24
5.2.1 Main WS_FTP Screen (WS_FTP Professional Version 2007)	25
5.2.2 Options Menu > Program Options (Program Options Version 2007).....	26
5.2.3 Example of Site Setup for SSLFTP WsFTP Professional Version 2007.....	28
5.2.4 Example of Site Setup for SFTP (WS_FTP Professional Version 7)	31
5.2.5 Certificate Screen (Version 2007)	34
5.2.6 Version WS_FTP Pro 2007 ENTRY IN SITE PROFILE ---.....	34
5.2.7 Example of Good Transfer Log.....	35
5.3 Connecting Issues.....	37
Section 6 - ACA CORE TRANSPORT MODES	38
6.1 Connectivity Overview	38
6.2 System Availability	38

6.3	Process Flows	39
6.3.1	Real-time Request and Response Handling.....	39
6.3.2	Batch Request and Response Handling	41
6.4	Transmission Administrative Procedures.....	44
6.5	Retransmission Procedures.....	44
6.6	Communication Protocols.....	44
6.6.1	HTTP MIME Multipart.....	44
6.6.2	SOAP + WSDL	44
6.6.3	Header Requirements.....	44
6.6.4	Error Reporting	46
6.7	Passwords.....	<u>4847</u>
Section 7 - ELECTRONIC BATCH WEB UPLOAD THROUGH CHAMPS		<u>5049</u>
Section 8 - B2B TESTING		<u>5453</u>
Section 9 - 999 Acknowledgement File.....		<u>5655</u>
Section 10 - APPLICATION ID/FILENAME.....		<u>6160</u>

Section 1 - INTRODUCTION

This Electronic Submission Manual describes how to submit data electronically to the Michigan Department of Community Health (MDCH). This manual explains how to communicate with MDCH via the Data Exchange Gateway (DEG) through a dial-up or Internet connection or SSLFTP connection or using the ACA CORE required SOAP+WSDL or HTTP/S MIME transport modes. It also provides instruction on how to submit transaction files directly into the CHAMPS web portal using Electronic Batch Web Upload through CHAMPS. Regardless of the method used to submit electronic Medicaid files, you must first test with MDCH.

This manual replaces all previous MDCH Electronic Submission Manuals.

Any entity that submits claims electronically to Michigan Medicaid is considered a billing agent for Michigan Medicaid. Billing agents can be software companies, providers, clearing houses, etc.

This manual will help all Medicaid billing agents in the submission of electronic files. If you do not have a billing agent ID, please review the Resources section of this manual.

There are several advantages to submitting claims and other data electronically:

- ❖ Electronic data reduces the need to re-type information;
- ❖ Electronic data eliminates the amount of errors;
- ❖ Electronic claims can be processed and paid much more quickly;
- ❖ Electronic claims can be posted more easily; and
- ❖ Electronic claims can be used for additional services, such as claim status information.

This manual will explain the necessary information for the actual transmission and receipt of electronic information. Only billing agents will be able to send and retrieve information to MDCH. **Any entity submitting 276 claim status requests has to be associated in CHAMPS with the Billing Agent or Trading Partner that originated the claim.**

Section 2 - RESOURCES

Many of the MDCH resources for electronic billing can be found at the MDCH website (such as: MDCH>>Providers>>Trading Partners>>*How to Become an E-biller*). Please make sure to review the resources available at this website before contacting MDCH directly. Resources that will be available at the MDCH website, including this Electronic Submission Manual, are:

- ❖ CHAMPS B2B Testing Instructions for 837 Fee for Service (FFS) & Encounters claims, NCPDP files, and 270, 276, and 278 Requests
- ❖ Electronic Updates
- ❖ Michigan Companion Guides
- ❖ 835 Electronic Remittance Advice Instructions
- ❖ 835 Change Request Form
- ❖ Approved Billing Agents Listing
- ❖ Links to additional Information about electronic Health Care transactions

EDI Services –

Michigan Medicaid EDI Department will handle all electronic questions related to FFS & Encounter file exchange and DEG problems.

Website:

www.michigan.gov/tradingpartners

Email:

AutomatedBilling@michigan.gov

Provider Inquiry Unit –

The Provider Inquiry Unit will handle all billing questions related to paper claims and the 837.

Website:

www.michigan.gov/mdch >> Providers >> Providers >> CHAMPS >>

Provider Inquiry Line:

1-800-292-2550

Email:

ProviderSupport@michigan.gov

Encounter Team -

The Encounter Team will handle questions on Billing.

Email:

MDCHEncounterData@michigan.gov

Section 3 - SOFTWARE AND PROGRAMMING

Michigan Medicaid does not provide software to billing agents for electronic claims submissions. All billing agents must have a way to create or produce electronic files to submit to Michigan Medicaid.

MDCH does have a posted “Approved Billing Agents” list at the Electronic Billing website. This will provide a list of billing agents that have completed the testing process and are in production status on behalf of other providers. It will also give contact information and status of billing agents that are willing to accept new providers. MDCH does not promote any one billing agent over another.

DRAFT

Section 4 - DATA EXCHANGE GATEWAY (DEG)

MDCH has established two communications connections for the DEG. The first connection, referred to as the dial-up connection, is a point-to-point protocol modem communications connection. The second connection, referred to as the Internet connection, is a Secure Sockets Layer connection. Both of these connections are independent of the platform used to transmit data.

Billing agents will use the DEG to submit and retrieve files electronically with MDCH. Every billing agent receives a “mailbox”, which is where their files are stored and maintained. You can access this mailbox to send and retrieve files through either the dial-up or Internet connection.

MDCH recommends that billing agents are able to connect through both the dial-up and Internet connection. You may decide which connection you prefer to use the majority of the time. MDCH cannot control the Internet or down phone lines and that is why it is important that providers become familiar with both ways to access the DEG

4.1 DEG - DIAL-UP CONNECTION

The dial-up connection is a two-part process which involves establishing a connection through the dial-up, and then establishing a connection with a file transfer protocol (FTP).

4.1.1 Hardware, Software and Connection Requirements

Transmitting Computer:	Any
Modem:	Up to 56 kilobytes per second
Software:	Both dial-up and FTP required once a connection is made into the DEG.
Dial-Up Number:	517-373-6181
TCP/IP address:	204.23.253.97

4.1.2 Dial-Up Specifications

The following instructions are provided as an example of how to establish a connection using Microsoft Windows software on a personal computer (PC). Since the dial-up connection does not depend on a particular platform or software, all of the possible methods of connecting cannot be addressed here. Figures are provided to help with the connection process. These instructions will only need to be done the first time to set up the connection. Once it is set up, you can go to the MDCH link that you are creating to log-in.

4.1.3 Setting up the MDCH Dial-Up Connection

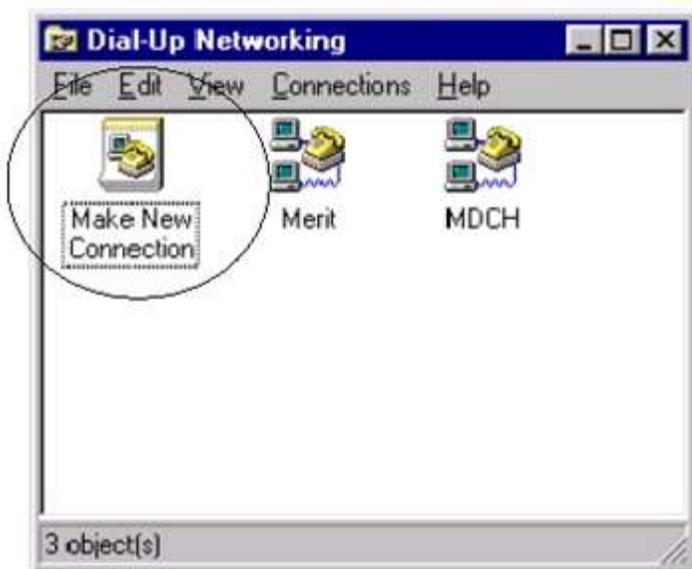
1. Double-click the “My Computer” icon on the computer desktop.



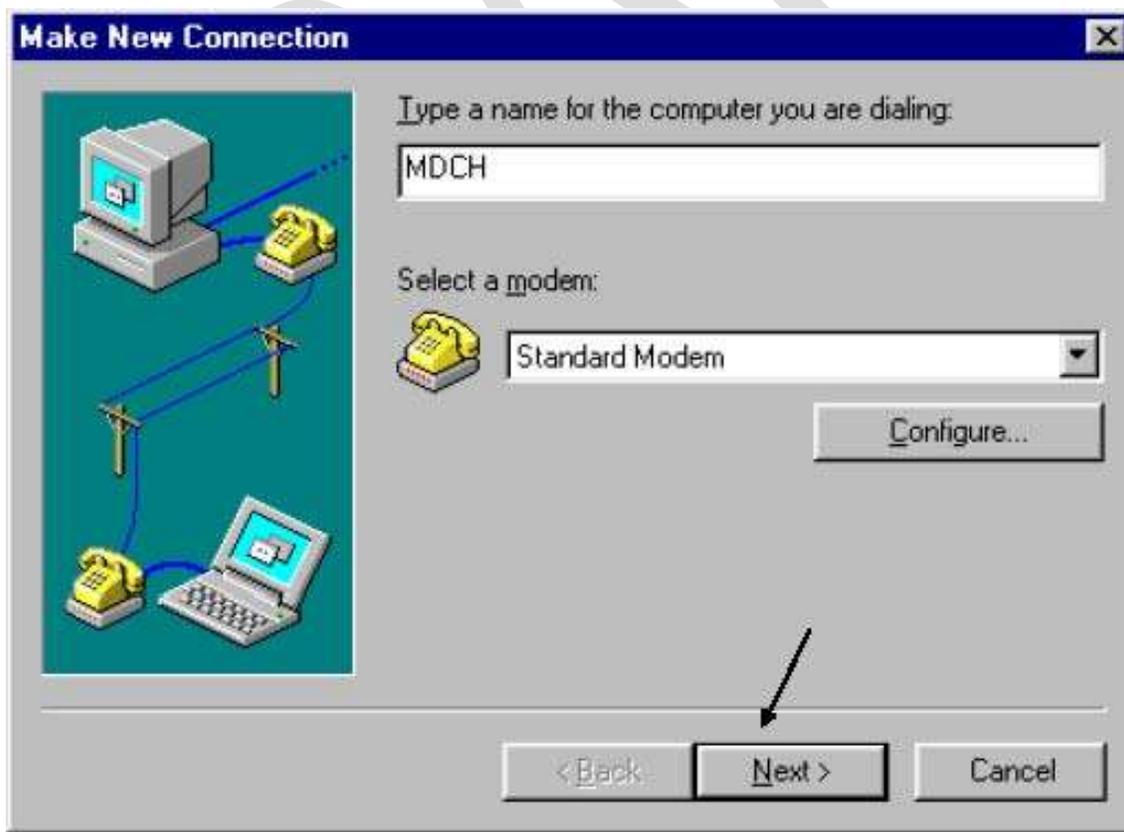
2. Double-click the “Dial-Up Networking” icon in the “My Computer” configuration window.



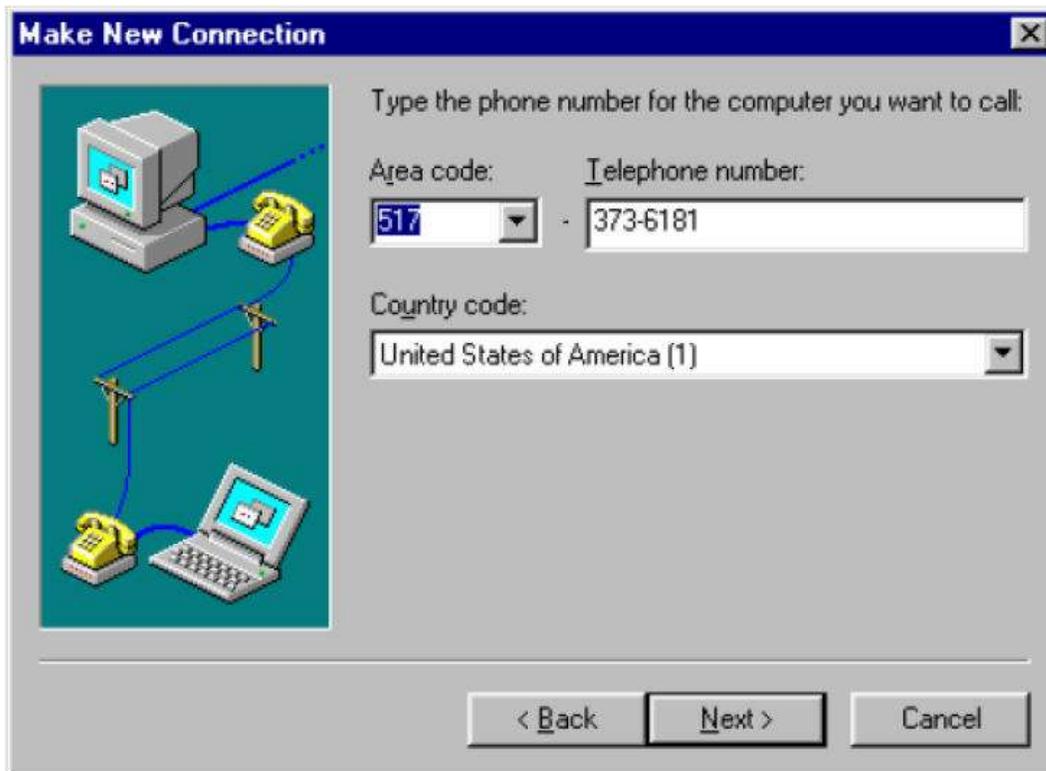
3. Double-click the “Make a New Connection” icon. The Make New Connection window appears. See figure below.



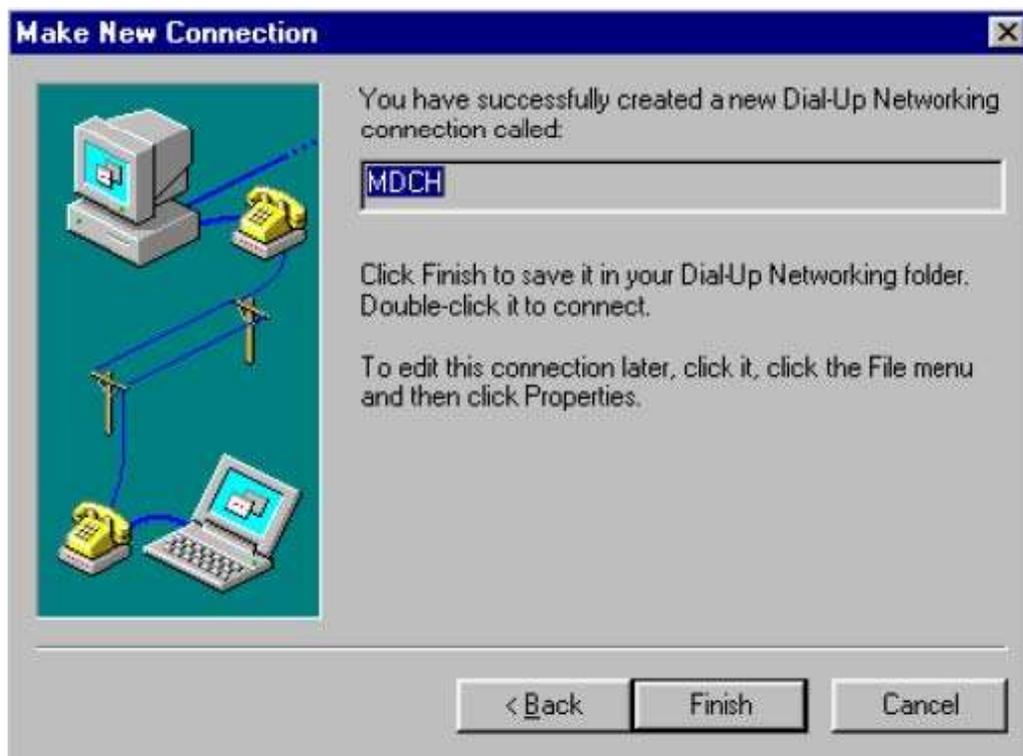
4. Enter **MDCH** in the first window and then select a modem or accept “Standard Modem”. Click “Next” when finished.



5. In the “Make New Connection” window, enter the area code **517** and telephone number **373-6181** in the appropriate fields; then enter **United States of America (1)** as the country code. Click “Next” when finished.



6. Click “Finish”. A new connection is established. The “Make New Connection” window automatically closes, and the connection appears in the “My Computer” window.

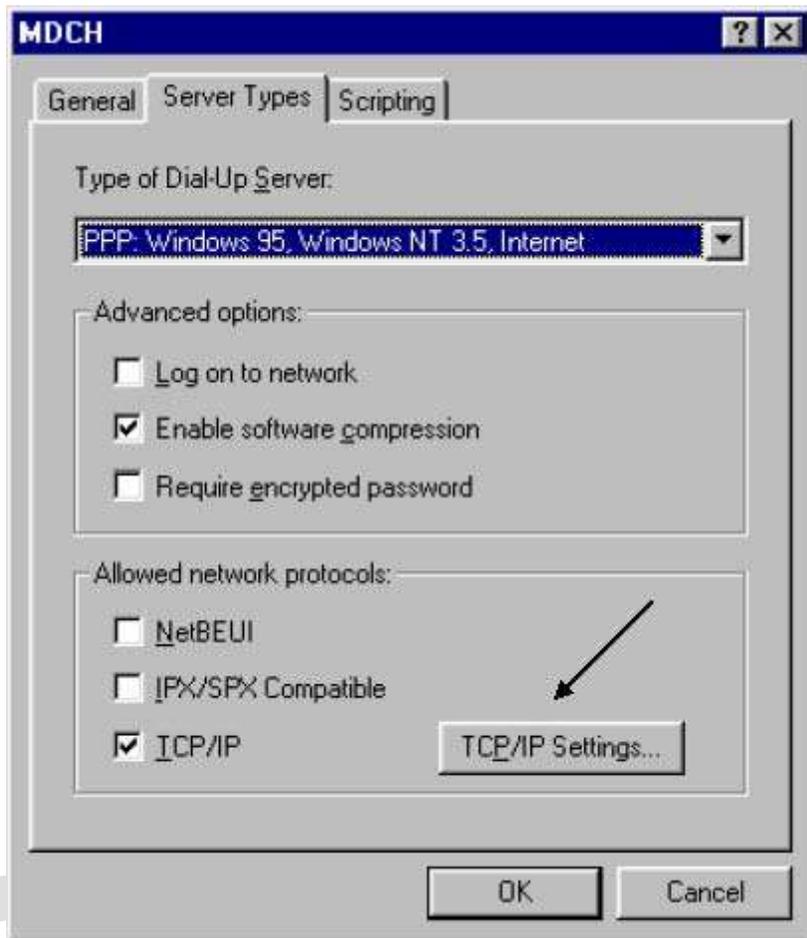


7. Return to the “Dial-Up Networking” window.
8. Select the MDCH icon just created by clicking on it once to select it.
9. Click “File” from the menu bar; then select “Properties” from the drop-down list.

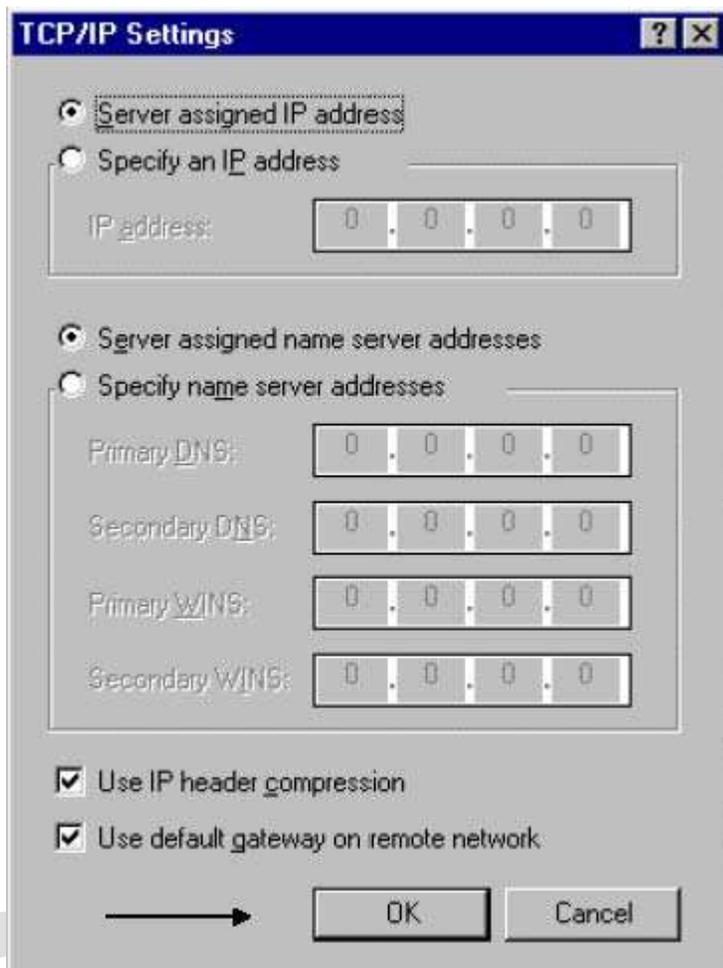
10. When the “MDCH” window appears, verify that the information is correct; then click the “Server Types” tab.



11. Select, "Type of Dial-Up Server" as "PPP: Windows 95, Windows NT 3.5, Internet". Then check the box next to "Enable software compression" by clicking in it once. Also check the "TCP/IP" box. Then click on the "TCP/IP Settings..." button.



12. Modify the window on the computer to look like the window in the figure below, and then click “OK”.



13. Click “OK” again to close the MDCH window. The dial-up connection is now ready.

4.1.4 Logging onto the MDCH Dial-Up Connection

1. Go to the Start Menu, and select Programs, Accessories, and Dial-Up Networking.
2. Double-click the MDCH icon.
3. The “Connect To” window appears.



4. Enter the user name and password of guest. This user name and password will establish that a connection has been made. Other user names and passwords are used for testing and production.
5. Verify that the correct telephone number appears in the correct field.
6. Click “Connect”.
7. Once the connection is established (the sounds of dialing and connection will be heard), the dial-up connection window minimizes itself.
8. Close the “Dial-Up Networking” window. You have now established a connection through the dial up.

4.1.5 FTP Specifications

The following example is based on the software that comes with Windows XP. It is similar to the DOS commands used by other operating systems. Other Windows-based FTP software is available.

1. To start an FTP session, click the Start Menu in the lower left corner of the computer screen.
2. Click "Run" from the Start Menu.
3. Enter ftp 204.23.253.97 in the open field, then click "OK".
4. Once the ftp software starts, a DOS window will appear. The DEG asks you for a user ID. Enter your billing agent ID as DCH00??, where 00?? represents the unique billing agent ID assigned by MDCH. Press the Enter key.
5. When prompted for a password, enter the password given for your billing agent ID, and press Enter.
6. Once the DEG responds, choose a command that allows you to transmit or download files. (See the section titled "FTP Commands" for commands.)
7. To end the FTP session, type bye.
8. To end the dial-up session, click the minimized "Dial-Up Networking" icon at the bottom of the screen. Click "Disconnect".

4.1.6 FTP Commands

Command	Description	Example
put	Move a file to the DEG	put<space><file location><space><application ID>@<destination ID> examples: put c:/filename 5475T@DCHEDI (to submit an 837 test file) put c:/filename 5475@DCHEDI (to submit an 837 production file)
dir	Show directory of files waiting for download	dir
get	Receive a file from the DEG	get<space><application ID><space><file location> example: get 4987 c:/filename (to retrieve an 835 file to your C:/ drive)
del	Delete a file from the DEG	del<space><application ID> example: del 5475 (to delete an 837 file - This will delete all files of this number!)
quit	End the FTP session	quit
help	Shows a list of commands	help
bye	Ends session	bye

File Naming Standards: Any file name that ends with a “T” will not be delivered to the production environment. A “T” designates a testing file. Please refer to the section in this manual titled “APPLICATION ID/FILENAME” for file naming requirements.

4.2 DEG - INTERNET CONNECTION

The Internet connection is the best PC setup to get the most reliable and fastest performance with DEG https Secure Internet File Transfer. Https provides for secure file transfer over the Internet. Https uses your Internet browser and provides secure connections.

4.2.1 PC Setup

1. You must have an Internet Browser installed on your PC. If you use Microsoft Internet Explorer, you must use version 6 or higher. You may use other web browsers as well. If you are not sure you have a browser installed, check with your PC technical support person. Internet Explorer 6 or later is included free on most Windows PCs.

Note that if you use a different web browser, some screens you see may be quite different than the screens you see in this documentation, which are based on Internet Explorer version 6.

2. Make sure you have a reliable Internet Service Provider (ISP) for your PC's Internet connection.
3. For the most reliable and fastest transfers, use a high-speed internet connection from your PC. This is a LAN, T1, DSL, or Cable connection to the internet. If your company already has such a connection, we strongly advise you to use it--almost always there's no added charge because this kind of connection has a flat monthly fee. If your PC has been dialing a phone number directly at the State, this high-speed connection has not been an option you could use. With https, you can use a high-speed connection if you have it. If you have no high-speed internet connection, getting one greatly speeds up all internet operations.
4. If you use a dial-up connection to the internet, we suggest that you use a 56K bps modem.
5. If you are using a dial-up connection, the version of Windows you are using will have an important effect on reliability. The Internet dial-up code included with Windows has made big improvements in later versions of Windows. For a dialup SSL FTP connection, the best version of Windows to use is Windows XP (or later). Windows 98 is preferred over Windows 95. Windows 95 is not acceptable unless a patch is downloaded.
6. We strongly recommend that you set your PC's screen to show a resolution of 800 x 600 pixels for readability. If you have a lower resolution (normally 640 x 480 pixels), you may have to scroll the screen horizontally; if you have a higher resolution (typically 1024 x 768 pixels) you will have some unused borders in a full-screen window.
7. Whether you use a dial-up or high-speed connections, for best performance, do not use an ancient PC. *However*, almost any PC is acceptable as long as it has a Pentium class processor or higher.

4.2.2 Logging onto the MDCH Internet Connection

- 1) Log into: <https://dxgweb.state.mi.us>

The screenshot shows the login interface for the Michigan Data Exchange Gateway. At the top left, it says "Official State of Michigan Portal" and "michigan.gov" with a state outline icon. At the top right, there is a "Change Password" link and the title "Data Exchange Gateway". The main heading is "Logon to Data Exchange Gateway". Below this are two input fields: "User:" and "Password:". A "Logon" button is positioned below the password field. A disclaimer states: "This State of Michigan computer system is for authorized acceptable use only. All actions are logged and monitored. Misuse may result in Federal and/or State criminal prosecution or civil penalties." At the bottom, there are logos for "DTMB Technology, Management & Budget" and "messagewaysolutions™ When every transaction counts".

- 2) In the User box, "Enter your User ID", you will enter your billing agent ID, such as DCH00?? all in caps, where the ?? is your unique number assigned by MDCH.
- 3) In the Password box, "Enter your Password", use your supplied MDCH password all in caps. Then click on the "Logon" button. After the first time you logon, it is suggested that you change your password to any unique combination or number or letters. Please make sure you save this new password and remember it because MDCH does not keep record of this password and will not be able to retrieve it.
- 4) If you need to have your password reset, please send a password reset request to: automatedbilling@michigan.gov

4.2.3 Downloading Files from the DEG

Downloading files allows billing agents to download files from their “mailbox”. These files can be TA1, 999 Acknowledgement files, 835 files, etc. Your available messages to download are displayed on the screen when you log on.

Official State of Michigan Portal
michigan.gov

Home | Change Password | Logout

Data Exchange Gateway

Mailbox: DCHTST1

Upload Available Msgs Downloaded Msgs Canceled Msgs Uploaded Msgs

						Rows 1/4 of 4	Previous	Next
	Message ID	Appl ID	Filename	Sender	Date/Time	Size		
X	20120406110538hduoan	4987	4987	DCHMMIS	Fri Apr 6 11:05:38 2012	60683		
X	20120406110416hdfsn	5475	5475	DCHMMIS	Fri Apr 6 11:04:16 2012	157		
X	20120406110313hdq1qa	5475	5475	DCHMMIS	Fri Apr 6 11:03:13 2012	287		
X	20120406110236hdp1ro	5475	5475	DCHMMIS	Fri Apr 6 11:02:36 2012	291		

Server Time: 11:05

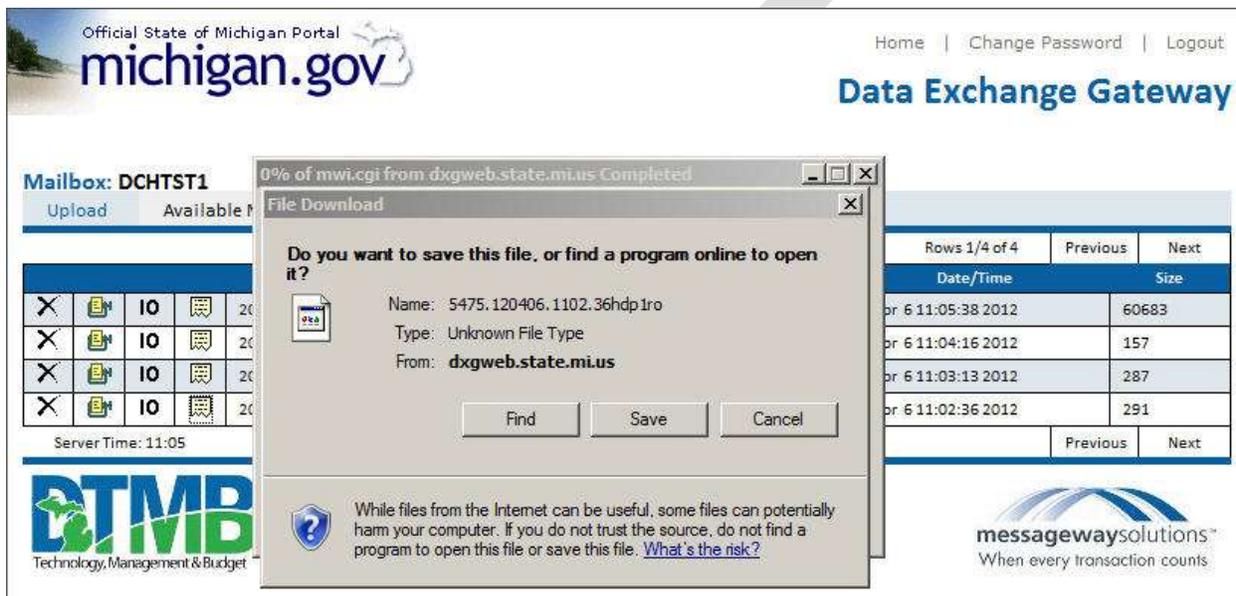
DTMB Technology, Management & Budget

messagewaysolutionsSM
When every transaction counts

Once a file is downloaded it will no longer appear on this page, you will need to click on **Downloaded Msgs** to view and/or re-download previously downloaded files.

-  This icon is for canceling files. You may cancel files you sent, located in the **Uploaded Msgs** area, or files sent to you in the **Available Msgs** area
-  This download icon is used if you are authorized to receive your data in a zip format. If so, you also need an unzip program on your PC and you are solely responsible for its proper use.
- IO** This download icon is used if you need to receive your data in a binary format.
-  This is the most commonly used download icon. It is used for .txt files.

1. Click on the download icon you're authorized to use for the file you want to download. The screen below will then appear. At this time make sure you choose "Save" and point the browser to the location on your PC's hard disk where you want to save the file you are downloading.
2. When the download is complete, you may open the file or choose to close the file and open the file later. The file may save in an unrecognizable format. You may have to manually choose to open the file in Notepad, WordPad, Microsoft Word, etc. Please check with your IT department for more information on this process.



4.2.4 Uploading Files to the DEG

Official State of Michigan Portal
michigan.gov

Home | Change Password | Logout

Data Exchange Gateway

Mailbox: DCHTST1

Upload Available Msgs Downloaded Msgs Canceled Msgs Uploaded Msgs

Rows 1/4 of 4 Previous Next

	Message ID	Appl ID	Filename	Sender	Date/Time	Size
X	20120406110538hduoan	4987	4987	DCHMMIS	Fri Apr 6 11:05:38 2012	60683
X	20120406110416hdrfsn	5475	5475	DCHMMIS	Fri Apr 6 11:04:16 2012	157
X	20120406110313hdq1qa	5475	5475	DCHMMIS	Fri Apr 6 11:03:13 2012	287
X	20120406110236hdp1ro	5475	5475	DCHMMIS	Fri Apr 6 11:02:36 2012	291

Server Time: 11:05 Previous Next

DTMB
Technology, Management & Budget

messagewaysolutions™
When every transaction counts.

1. To start the Uploading process, click on **Upload**. The screen below will then appear.

Official State of Michigan Portal
michigan.gov

Home | Change Password | Logout

Data Exchange Gateway

Mailbox: DCHTST1

Upload Available Msgs Downloaded Msgs Canceled Msgs Uploaded Msgs

Upload Message

Mailbox:

Application ID:

Transfer Mode: Binary Text

File:

Warning: Do not exit this page while upload in progress...partial upload will result

DTMB
Technology, Management & Budget

messagewaysolutions™
When every transaction counts.

- **Mailbox** will be DCHEDI for most files that you are uploading to MDCH.
 - **Application ID** is the MDCH File Name of the file that you are submitting. Please see the section titled “APPLICATION ID/FILENAME” for a listing of application ID/File Names.
(ex. **5475** is the application ID for 837 FFS files)
 - **Transfer Mode** is normally set to text for most files submitted.
 - **File** is the file that you are submitting to MDCH through the DEG. You will need to click on the **Browse** button to attach the file that is saved on your PC.
2. When completed, click on **Upload** to submit the file
 3. Once the upload has completed, the following message will appear across the bottom of the upload screen.

**Message 20110211122138op8366 successfully uploaded
from DCH00xx to DCHEDI**

NOTE: This is not your 999 acknowledgement file. If you are submitting a file to MDCH and would like to verify your return acknowledgement file, you will have to go to **Available Msgs** to verify that your 999 acknowledgement file has been returned for each file that you sent. The Application ID or Filename of your 999 is the same Application ID of the file you sent. (Example: An 837 claims file submitted as 5475 would receive a 999 acknowledgment file also called 5475.)

Section 5 - SSLFTP/SFTP (WS_FTP) SETUP FOR THE DEG

5.1 Overview

This section provides information on how to set up your SSLFTP/ SFTP client software to use with the State of Michigan Data Exchange Gateway (DEG). It is not a user manual on how to setup SSLFTP clients; we cannot cover all possible software that can be used as a client. This section gives the basic information needed for a user who is knowledgeable in the use of their SSLFTP/SFTP client software to set up their client.

The following example shows how to set up the WS_FTP PRO 2007 SSLFTP/SFTP client to use with the DEG. It is an example of how the setup information may be entered in a client software package. It is not a WS-FTP user guide or even a WS-FTP setup guide. The example setup is configured to use SSL.

Use IP address 136.181.135.38

SSLFTP is port 11250 and data port 11200-11240

Note: You may need to open ports 11200-11240 in your firewall. SFTP is port 2222.

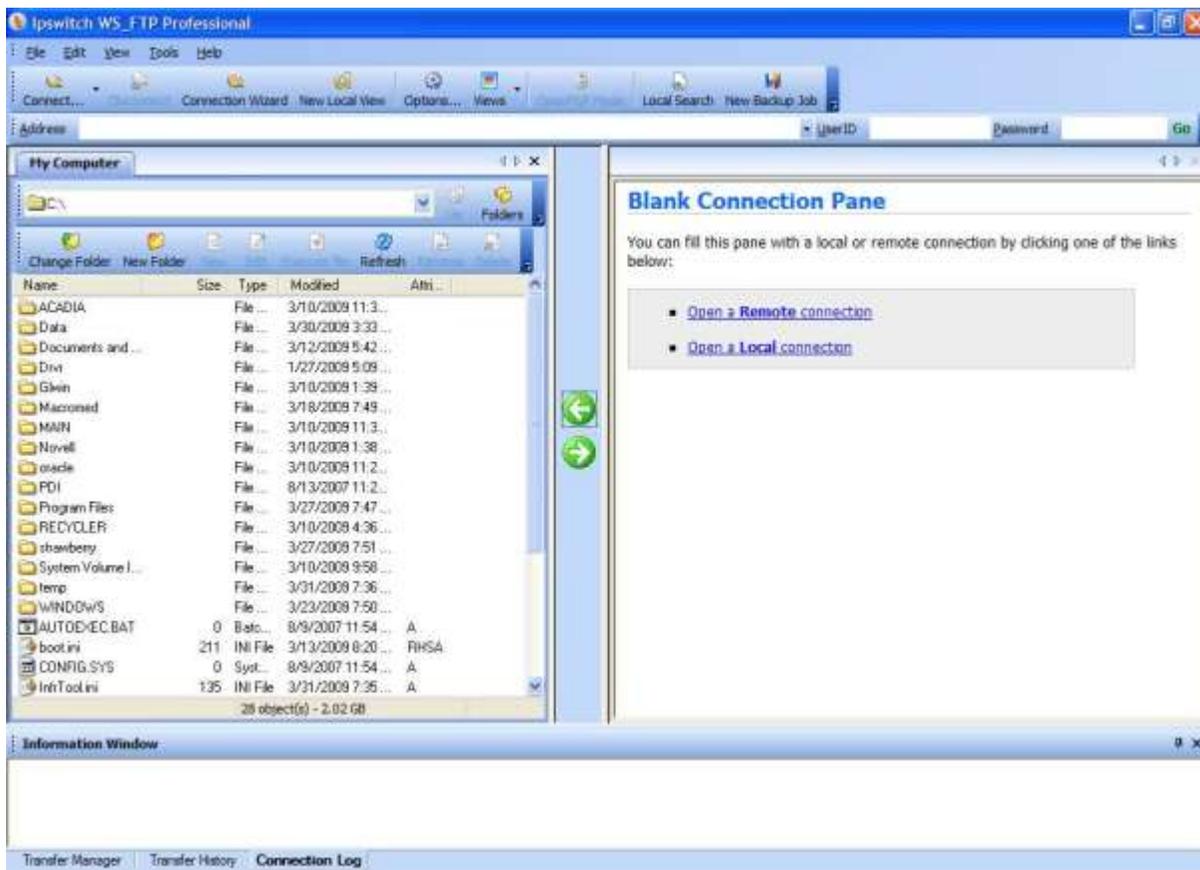
5.2 WS_FTP Pro Version 2007

You will need a WS_FTP version that supports SSLFTP/SFTP.

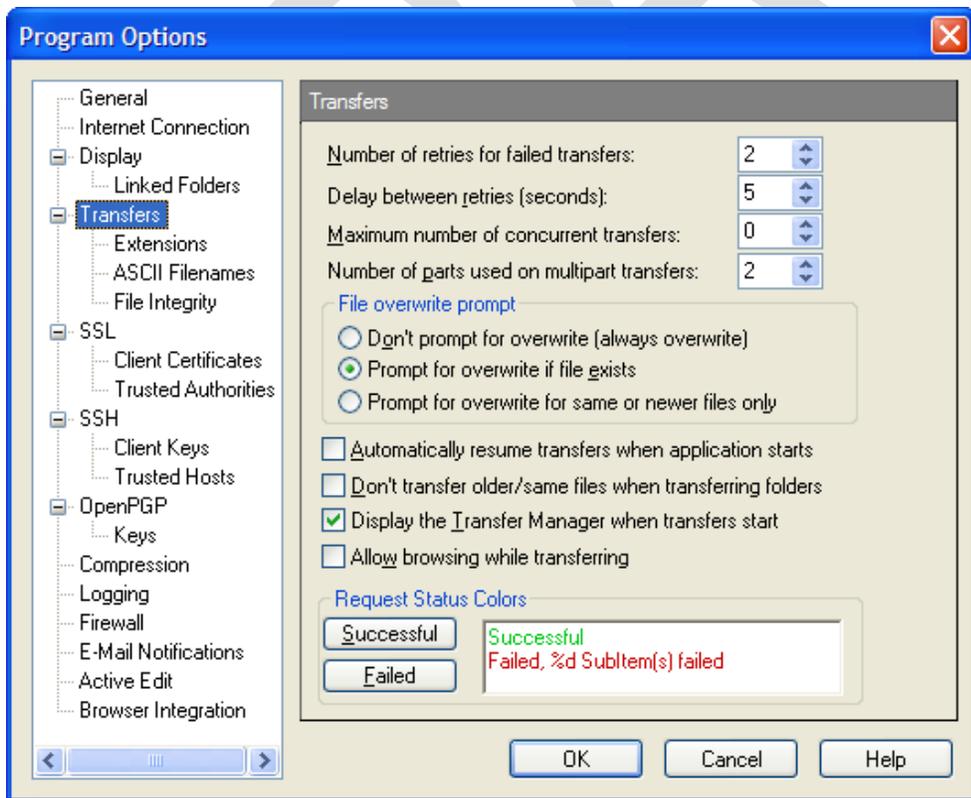
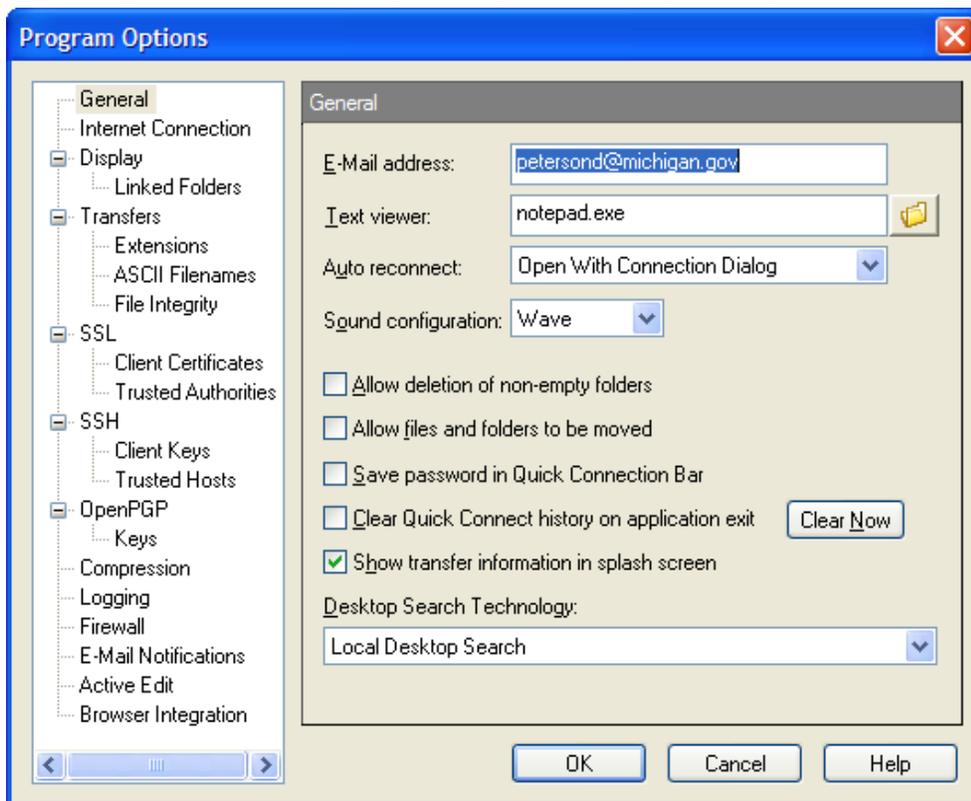
NOTE about Passwords:

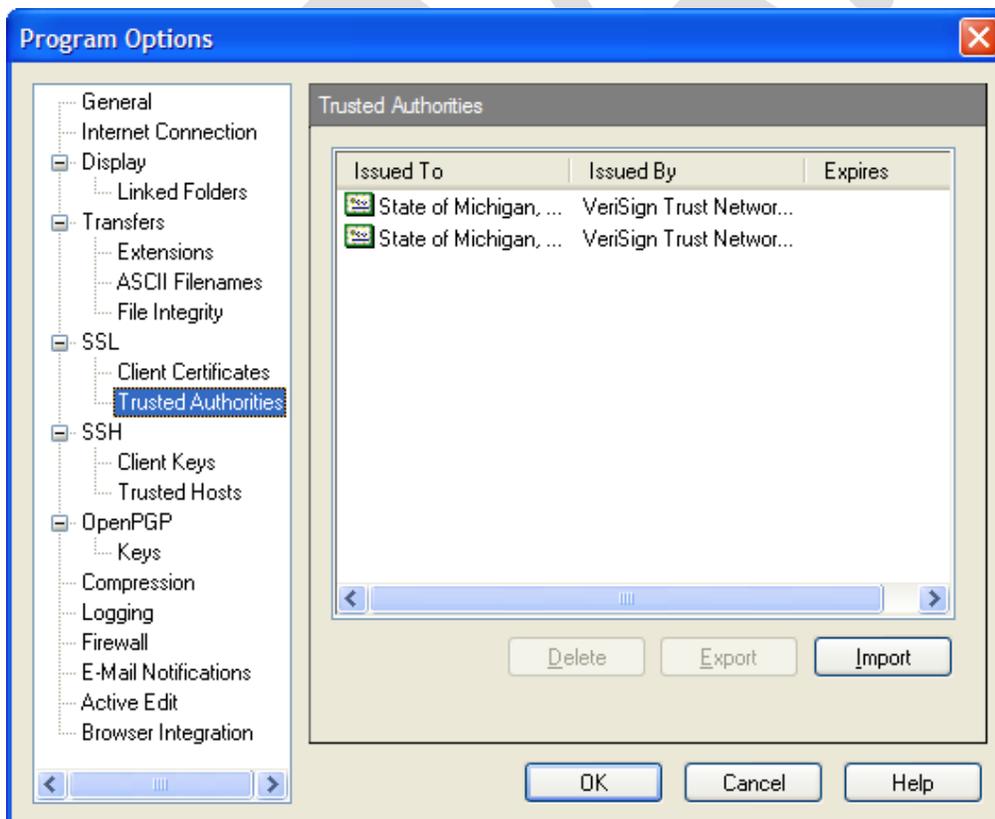
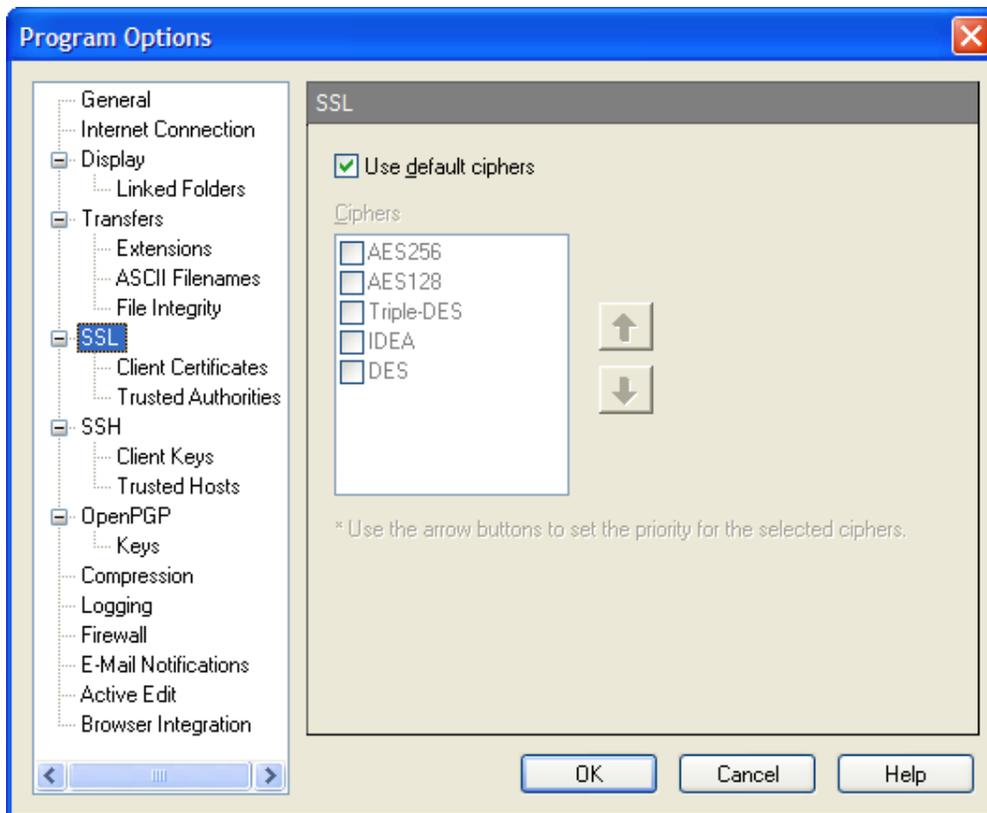
Currently all passwords are converted to upper case, regardless of what is entered. Please enter all passwords in Upper Case. In the future the DEG passwords may become case sensitive in which case, a password entered with lower case will fail to match the stored password. If you always use an upper case password until notified that lower case passwords are usable, then you will not have any problems when there is a change. This is very important if you are automating your connection with a program or script file.

5.2.1 Main WS_FTP Screen (WS_FTP Professional Version 2007)

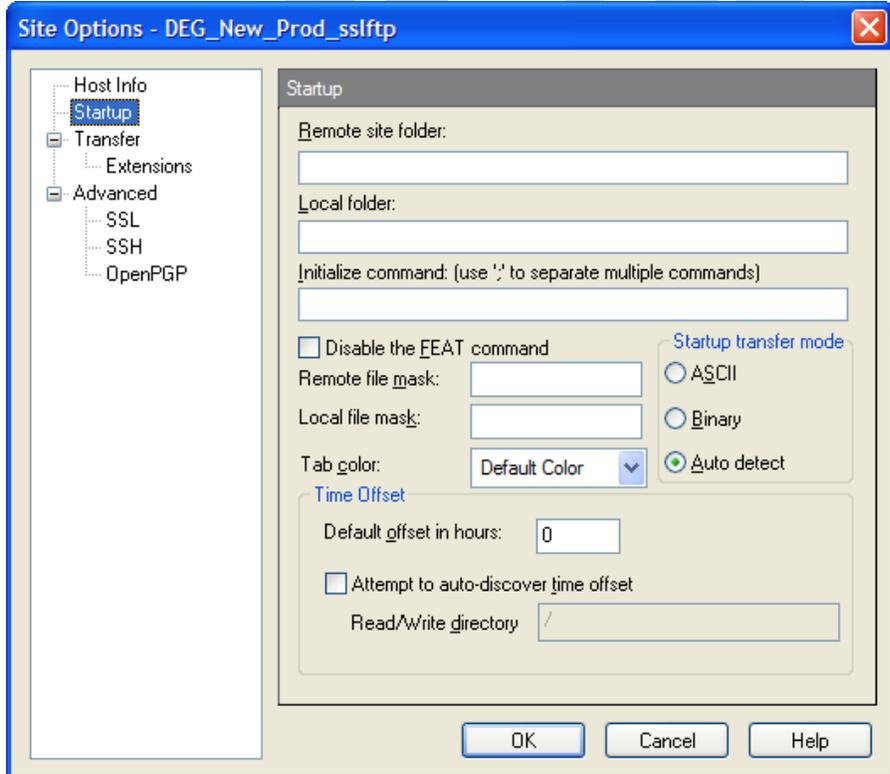
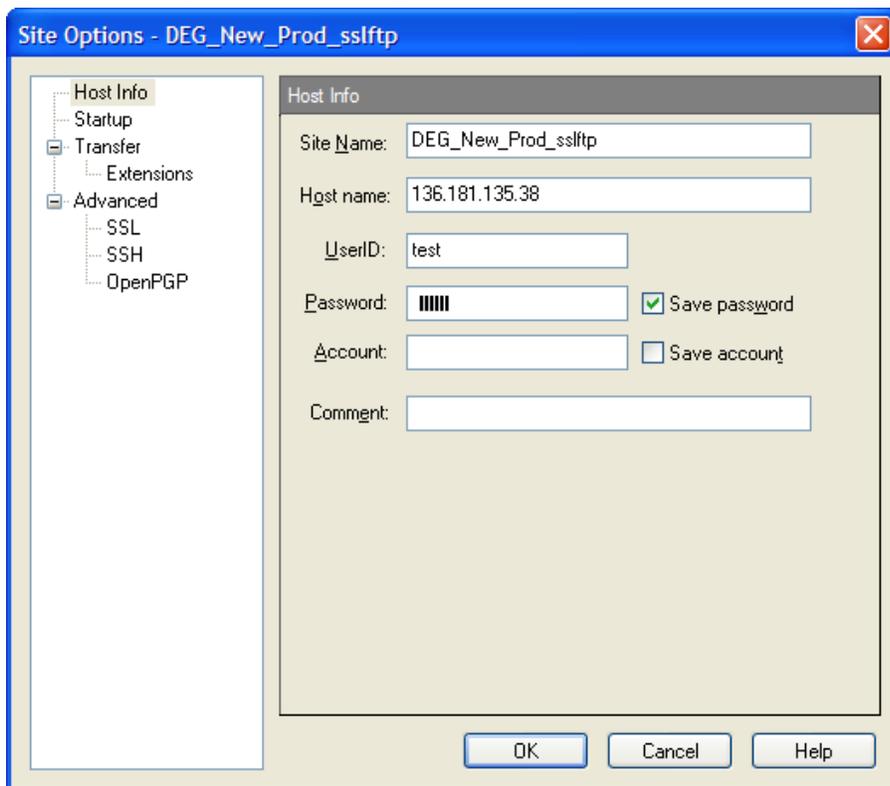


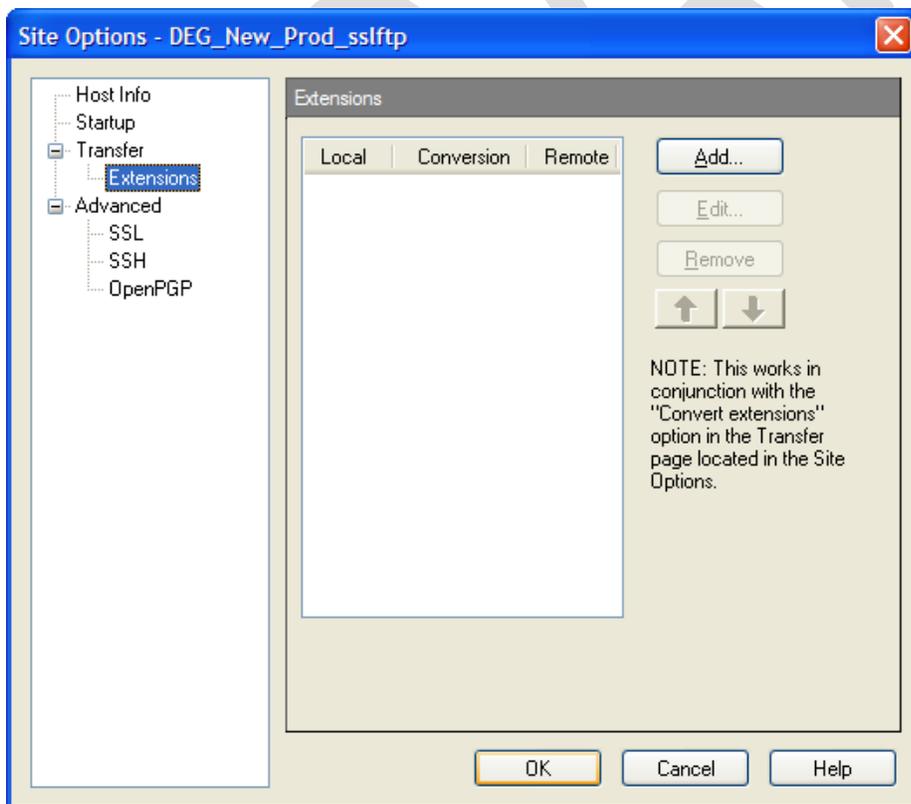
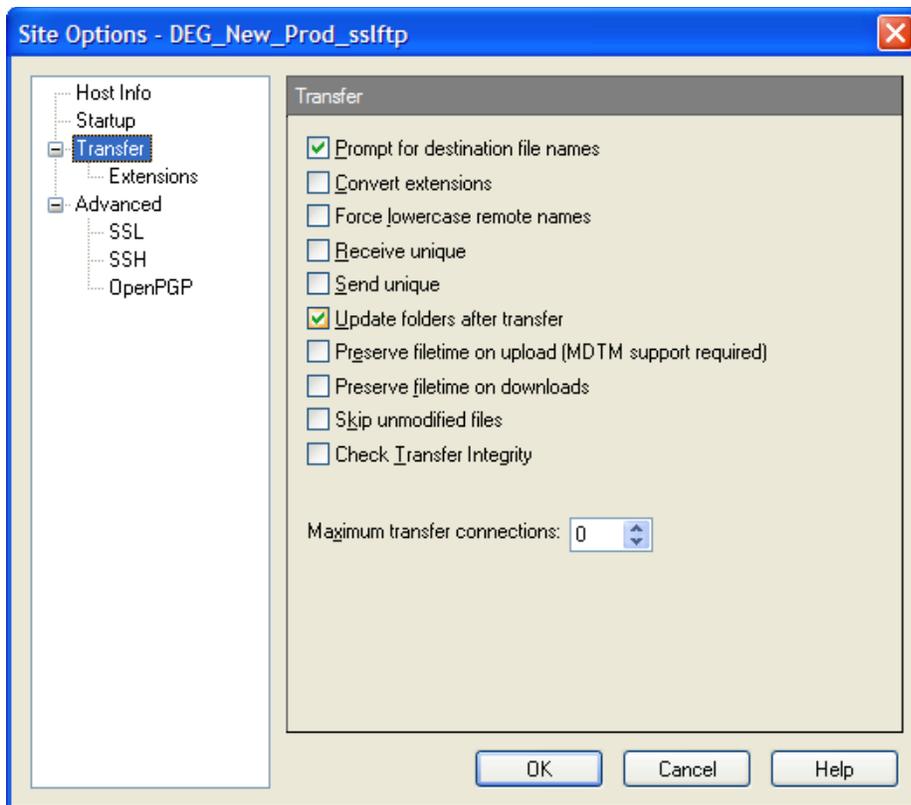
5.2.2 Options Menu > Program Options (Program Options Version 2007)

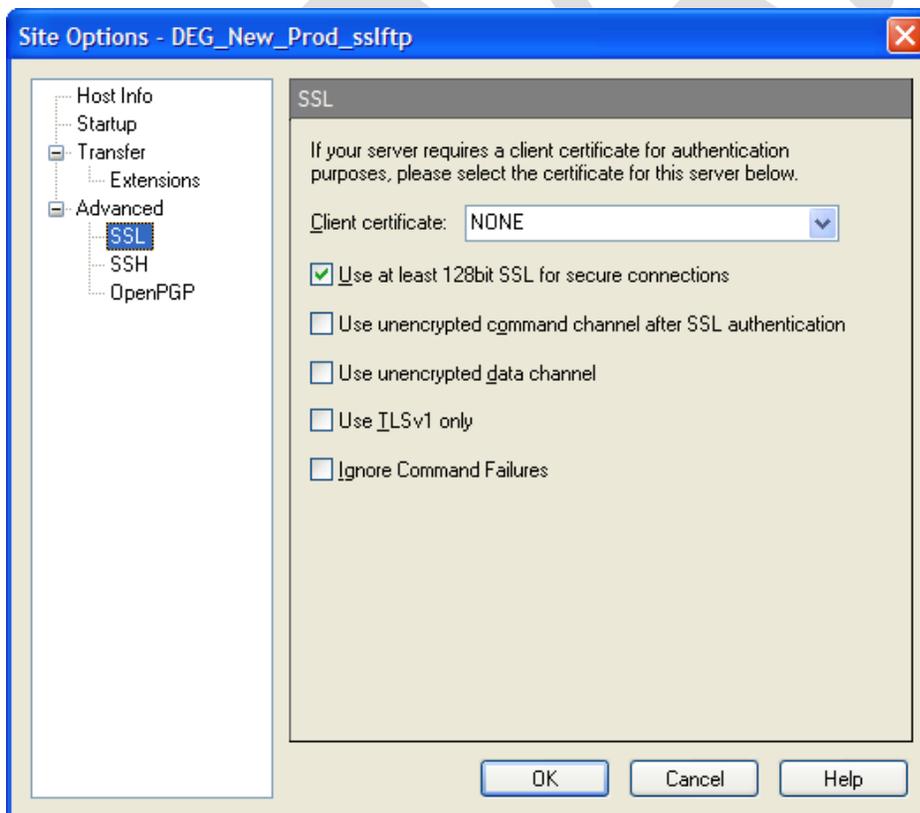
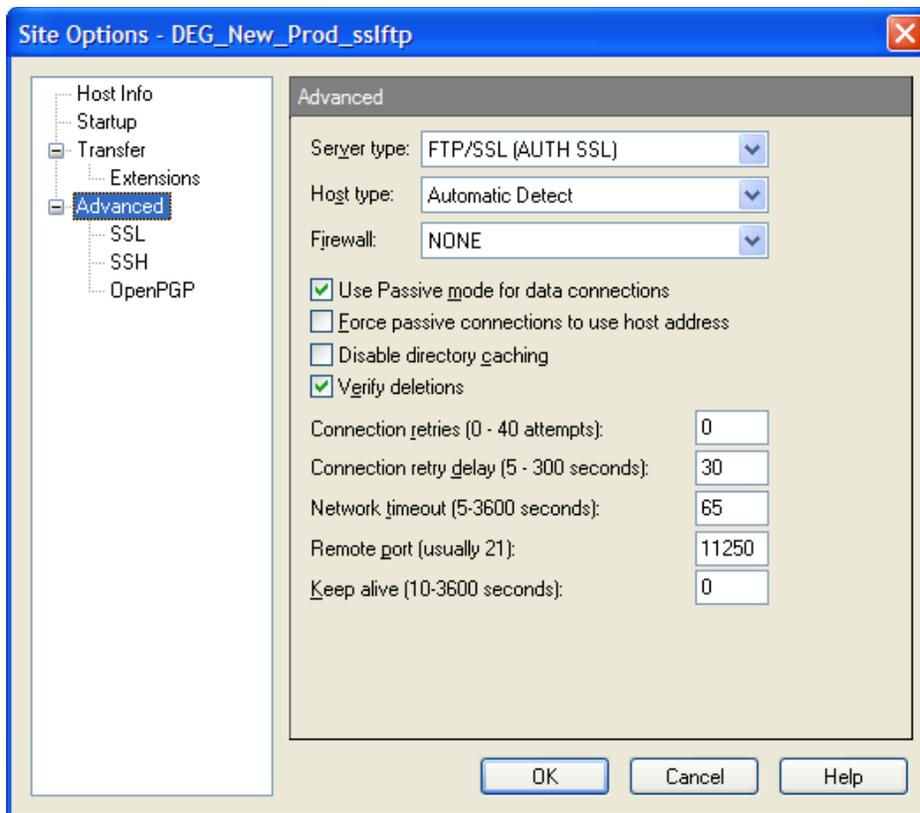




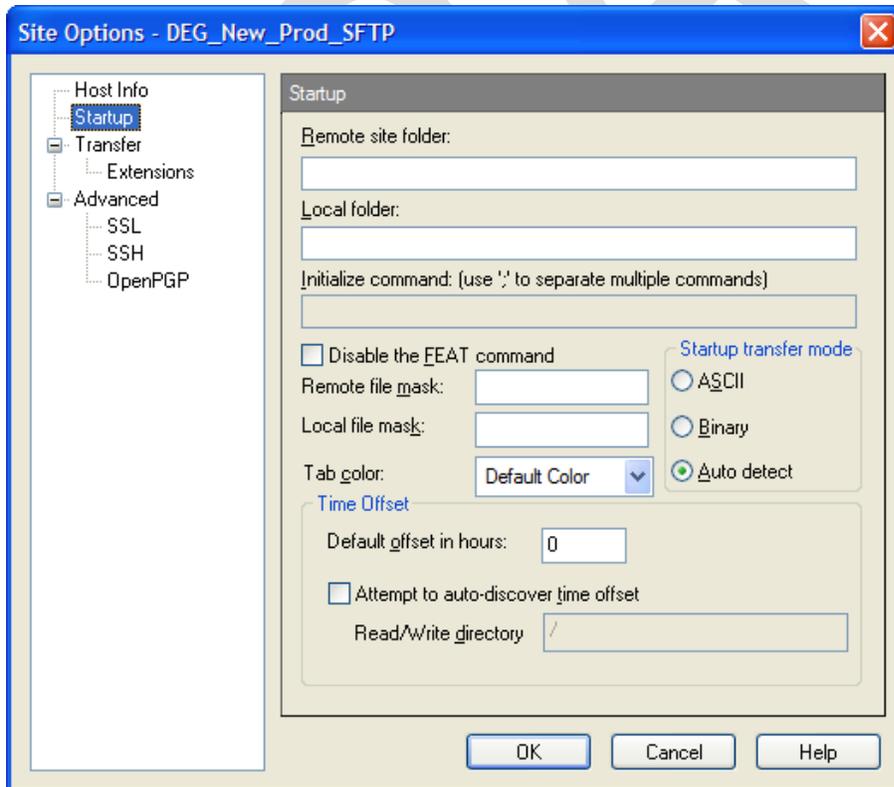
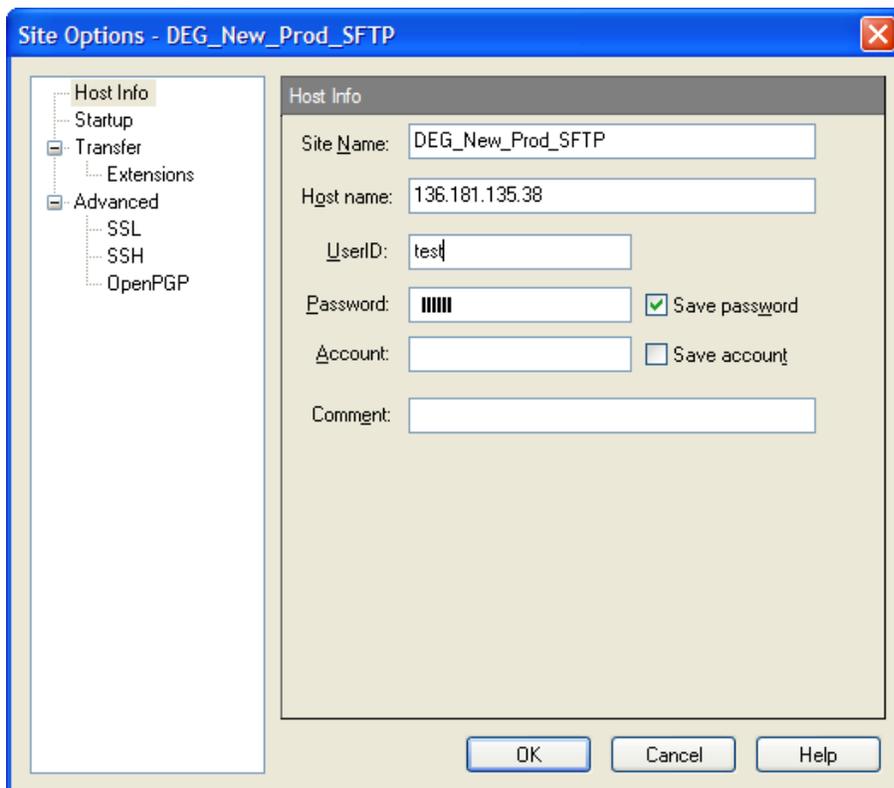
5.2.3 Example of Site Setup for SSLFTP WsFTP Professional Version 2007

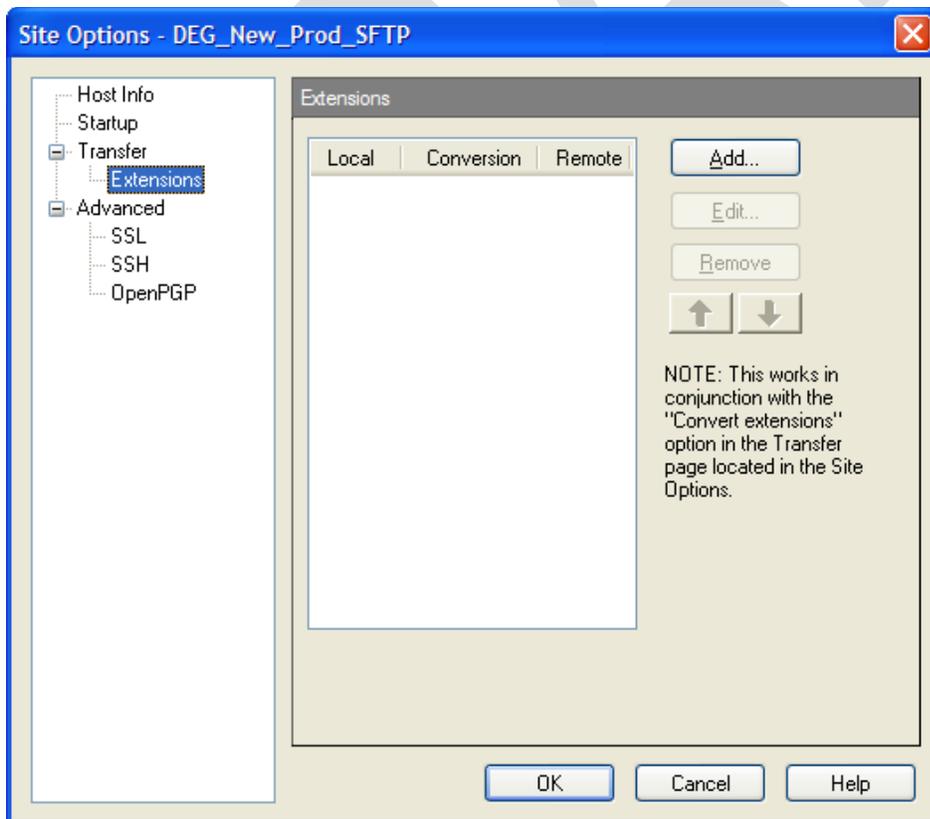
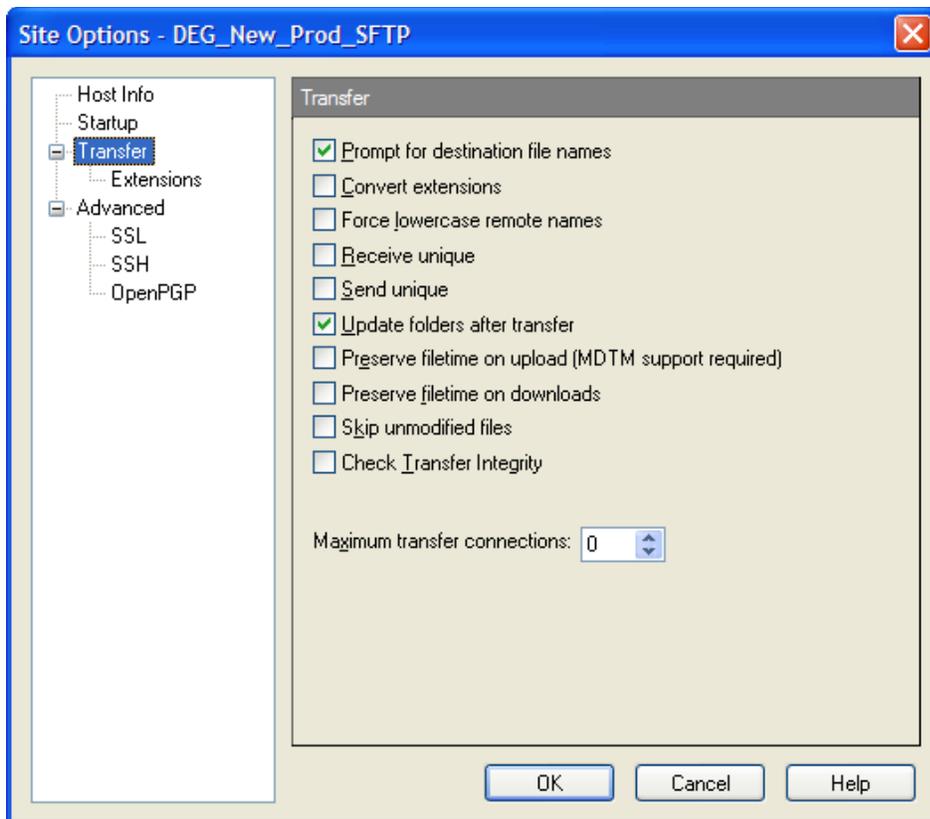


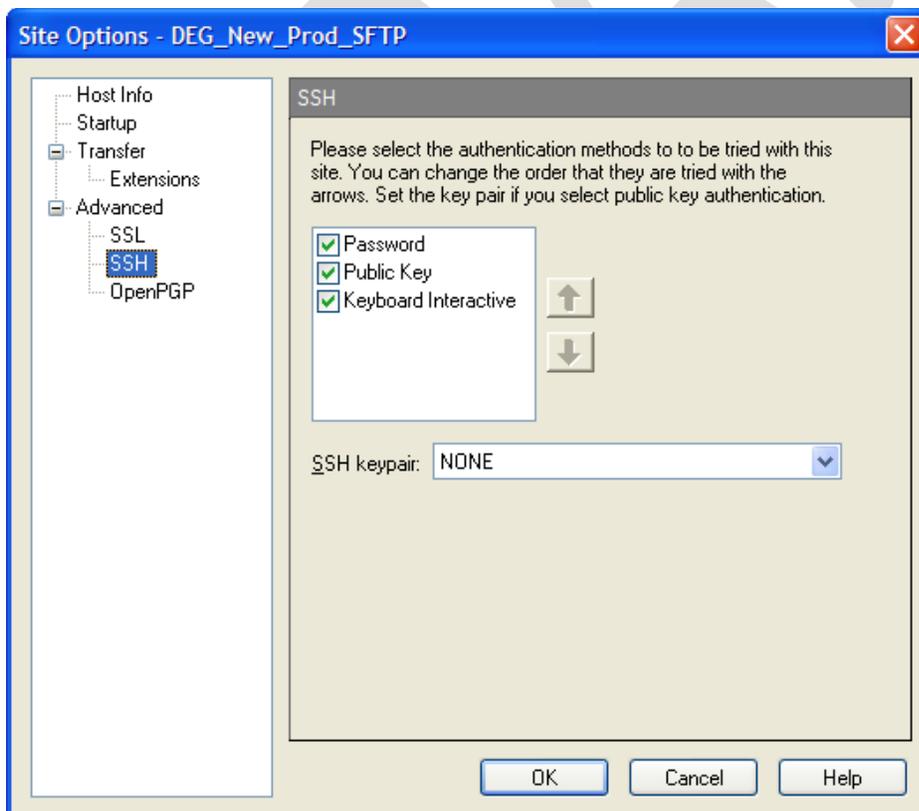
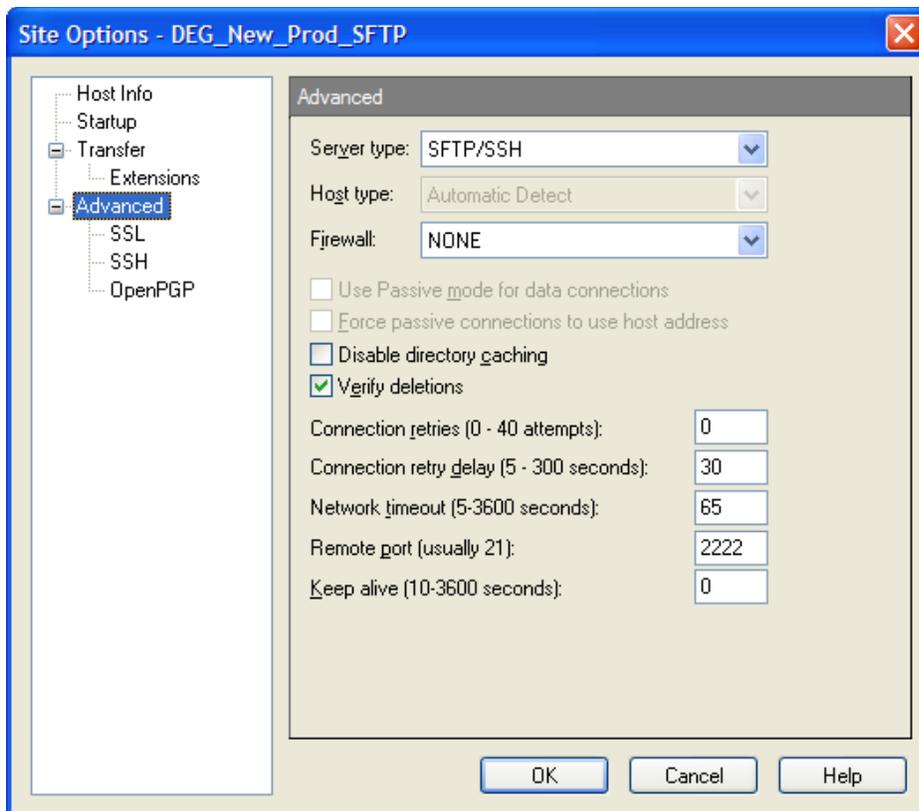




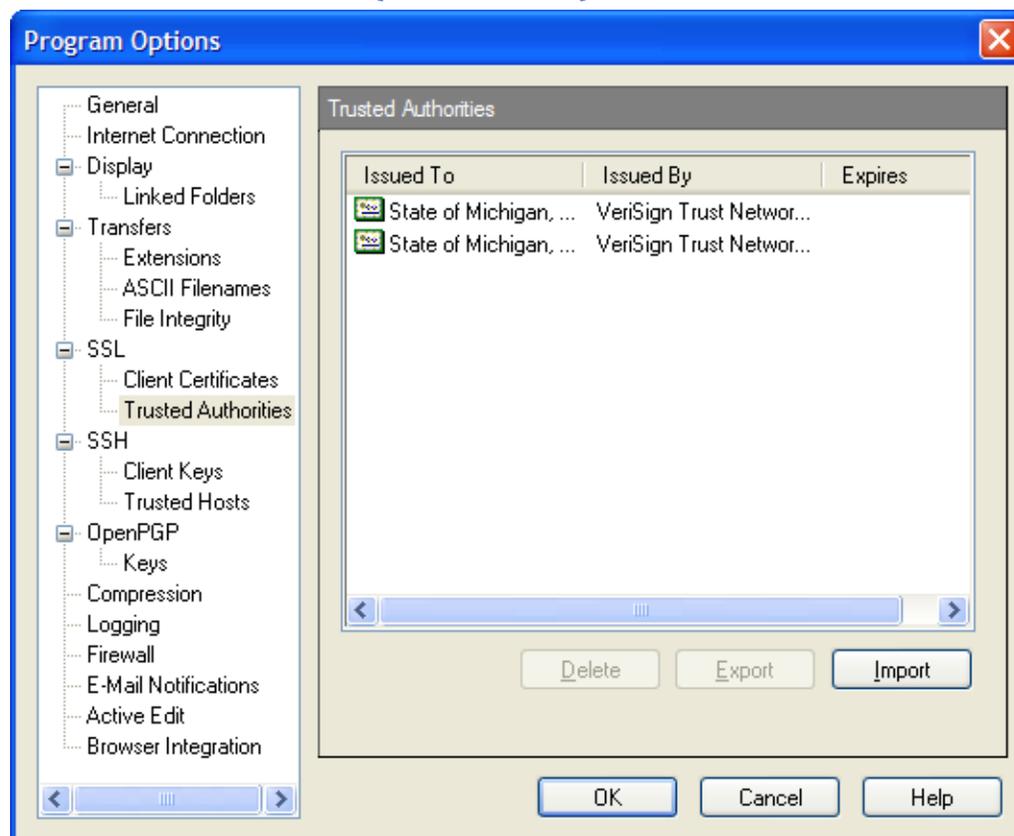
5.2.4 Example of Site Setup for SFTP (WS_FTP Professional Version 7)







5.2.5 Certificate Screen (Version 2007)



5.2.6 Version WS_FTP Pro 2007 ENTRY IN SITE PROFILE ---

On Windows 2000 and Windows XP: c:\documents and settings\username\application data\lpswitch\Ws_ftp\Sites\ws_ftp.ini

```
[_config_]
mailaddr=test@michigan.gov
URLHistory=urhistory.ini
dir0=c:\Data
[DEG_New_Prod_sslftp]
CONNTYPE=5
HOST="136.181.135.38"
UID="test"
PWD="_W+J7jLDGxlrwcZY+6xr0ZYOmIP1TYiKRI3Ktd6R8="
TABCOLOR="default"
AutoTimeOffsetPath="/"
1033ConvertDirListFrom=0
1033ConvertASCIIDownloadFrom=0
1033ConvertASCIIUploadTo=0
Use128bitSSLAtLeast=1
ClearCommandChannel=0
ClearDataChannel=0
RETRIES=0
PORT=11250
PROMPT=1
PGPENCODETYPE=0
firename="NONE"
dir0=/ftpst2a
dir1=/tmpuser
[DEG_New_Prod_SFTP]
```

Electronic Submissions Manual

```
CONNTYPE=4
HOST="136.181.135.38"
UID="test"
PWD="_INLDQIYXrFUYeG142fG1V_gLMeAw"
TABCOLOR="default"
AutoTimeOffsetPath="/"
1033ConvertDirListFrom=0
1033ConvertASCIIIDownloadFrom=0
1033ConvertASCIIUploadTo=0
filename="NONE"
RETRIES=0
PORT=2222
PASVMODE=0
PROMPT=1
PGPENCODETYPE=1
dir0=/ftpst2a
Use128bitSSLAtLeast=1
ClearCommandChannel=0
ClearDataChannel=0
TIMEOFFSET=0
UseAutoTimeOffset=0
TYPE=6000
UploadStatPeriod=0
DownloadStatPeriod=0
aborseq=0
TIMEOUT=65
CommandTimeout=60
AborTimeout=10
RETRYDELAY=30
RBP=0
SBP=0
KEEPALIVE=0
PREASKPASS=0
NOCACHEAUTH=0
NOCACHEDIRS=0
AUTORECONNECT=1
PRESERVETIMEUP=0
PRESERVETIMEDOWN=0
nofeat=0
TRANSFERCONN=0
DATAPORT=0
AMODE=1
MODE=73
CONVEXT=0
DOUPDATE=1
FORCLOW=0
NOTRANSLATEDATAIP=0
STOU=0
RECU=0
VRFYDEL=1
ENABLEPGPMODE=0
ENABLECOMPRESSION=0
CHECKTRANSFERINTEGRITY=0
FORCEPASVTOHOST=0
TRANSFERBATCH=0
TRANSFERMULTIPART=0
TRANSFERAPEND=0
```

5.2.7 Example of Good Transfer Log

SSLFTP Transfer Log Example

```
Connecting to 136.181.135.38:11250
Connected to 136.181.135.38:11250 in 0.000000 seconds, Waiting for Server Response
Initializing SSL Session ...
220 DEG FTPS. WARNING: UNAUTHORIZED USE PROHIBITED. ALL USERS ARE LEGALLY ACCOUNTABLE FOR
THEIR ACTIONS. BY USING THIS SYSTEM, YOU CONSENT TO HAVING YOUR ACTIONS LOGGED.
AUTH TLS
```

Electronic Submissions Manual

234 AUTH: securing command channel
SSL session NOT set for reuse
SSL Session Started.
Host type (1): Automatic Detect
USER test
331 Password Required
PASS (hidden)
230 Logon Accepted
SYST
215 UNIX Type:L8
Host type (2): Unix (Standard)
PBSZ 0
200 PBSZ: set for streaming mode
PROT P
200 PROT: data channel in PROTECTED mode
Sending "FEAT" command to determine what features this server supports.
FEAT
211-Extensions supported
211- AUTH TLS|SSL
211- CCC
211- PBSZ 0
211 PROT P|C
Finished interpreting "FEAT" response.
Sending the FEAT command is optional. You can disable it in the site options of the profile.
PWD
257 "/ftpst2a"
TYPE A200 Transfer Mode: ASCII
PASV
227 Entering PASV Mode (136.181.135.38,43,193)
connecting data channel to 136.181.135.38:43,193(11201)
data channel connected to 136.181.135.38:43,193(11201)
LIST
150 Connecting Data Port...
transferred 1040 bytes in 0.078 seconds, 106.496 kbps (13.312 kBps), transfer succeeded.
226 Listing Complete
Starting request
Sending "REST" command to determine if the server supports restarts.
REST 1024
502 REST: Command Not Implemented
This server does not appear to support restarts.
-- Resuming of interrupted transfers disabled.
-- Multipart downloads disabled.
Finished checking for "REST" command support.
TYPE I
200 Transfer Mode: BINARY
PASV
227 Entering PASV Mode (136.181.135.38,43,194)
connecting data channel to 136.181.135.38:43,194(11202)
data channel connected to 136.181.135.38:43,194(11202)
STOR test45
150 Connecting Data Port...
226 Stored Message: [200903311002330013rs] Size: [1131781] bytes
transferred 1131781 bytes in 0.813 seconds, 11143.690 kbps (1392.961 kBps), transfer succeeded.
Transfer request completed with status: Finished
TYPE A
200 Transfer Mode: ASCII
PASV
227 Entering PASV Mode (136.181.135.38,43,195)
connecting data channel to 136.181.135.38:43,195(11203)
data channel connected to 136.181.135.38:43,195(11203)
LIST
150 Connecting Data Port...
transferred 1117 bytes in 0.078 seconds, 114.381 kbps (14.298 kBps), transfer succeeded.
226 Listing Complete

SFTP Transfer Log Example

```
Connecting to 136.181.135.38:2222
Connected to 136.181.135.38:2222 in 0.000000 seconds, Waiting for Server Response
Server Welcome: SSH-2.0-OpenSSH_4.3
Client Version: SSH-2.0-WS_FTP-2007.1-2007.11.12
DSS Signature Verified
Session Keys Created
Ciphers Created
New Client->Server ciphers in place.
New Client->Server ciphers in place.
Completed SSH Key Exchange. New Keys in place.
Trying authentication method: "password"
User Authenticated OK!
Completed SSH User Authentication.
Started subsystem "sftp" on channel 0760a2ce
SFTP Protocol Version 3 OK
sftp protocol initialized
Getting Dirlistingtransferred 2187 bytes in 0.016 seconds, 1119.737 kbps ( 139.967 kBps), transfer succeeded.
Starting request
Opening remote file "/ftpst2a/test45" for writing
Uploading local file "c:\Data\test45"
transferred 1131781 bytes in 1.391 seconds, 6510.878 kbps ( 813.860 kBps), transfer succeeded.
Transfer request completed with status: Finished
Getting Dirlisting
transferred 2337 bytes in < 0.001 seconds, 18696.000 kbps ( 2337.000 kBps), transfer succeeded.
```

5.3 Connecting Issues

1. If you can't logon with SSLFTP, make sure you have the right port number 11250 and advance – server type select – FTP/SSL (AUTH SSL) or with SFTP, make sure you have the right port number 2222 and advanced – server type select – SFTP/SSH.
2. If you are getting a logon OK , but don't get a directory back from your mailbox, you are having a problem with the return data port 11200. First try turning on **PASSIVE MODE**; if that doesn't work, you may have a problem with your firewall.
3. If you get an error and you try automatically again, you might want to edit your site profile and make **AUTOCONNECT = 0** and **RETRIES = 0**. See above in document.

Section 6 - ACA CORE TRANSPORT MODES

6.1 Connectivity Overview

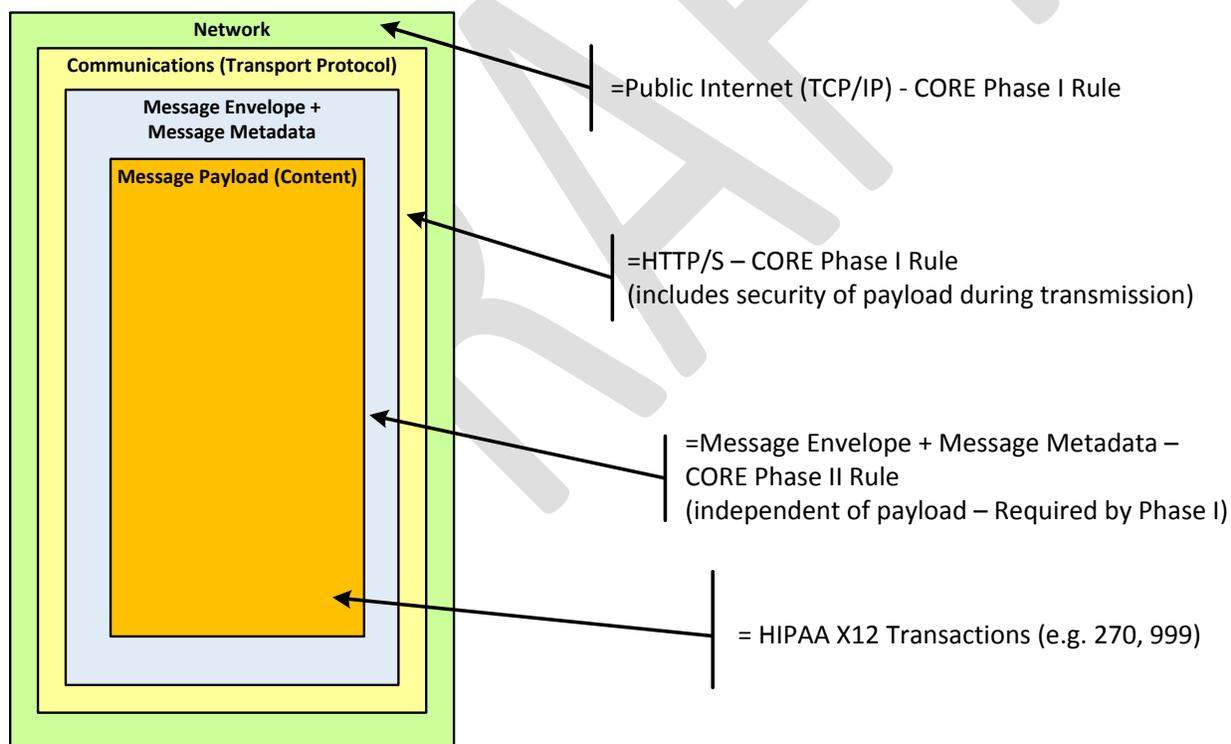
As part of the ACA CORE requirements, CHAMPS supports batch and real-time transmission modes and the following envelope standards for the 270/271 and 276/277 transaction sets.

1. HTTP MIME Multipart (Envelope Standard A)
2. SOAP+WSDL (normative) (Envelope Standard B)

Please refer to the CORE 270: Connectivity rule document at the link below for detailed information about the specifications for HTTP MIME Multipart and SOAP+WSDL based interactions.

<http://www.caqh.org/pdf/CLEAN5010/270-v5010.pdf>

The following diagram depicts the relationship of the transport modes to the submitted transaction.



6.2 System Availability

The MDCH CHAMPS system is available 24 by 7 with the exception of a regular monthly maintenance window, which starts at 6pm on the second Saturday of each month and ends at 6am on Sunday. For information on unscheduled outages, please check the Biller "B" Aware

page at the following link.

http://www.michigan.gov/mdch/0,1607,7-132-2945_42542_42543_42546-101427--,00.html#Biller_B_Aware

A response to the real-time inquiry will be provided within 20 seconds during hours of availability.

The v5010 271 response to a v5010 270 batch inquiry submitted by 9:00 pm Eastern time of a business day will be returned by 7:00 am Eastern time the following business day. Similarly, a v5010 277 response to a v5010 276 batch inquiry submitted by 9:00 pm Eastern time of a business day will be returned by 7:00 am Eastern time the following business day.

6.3 Process Flows

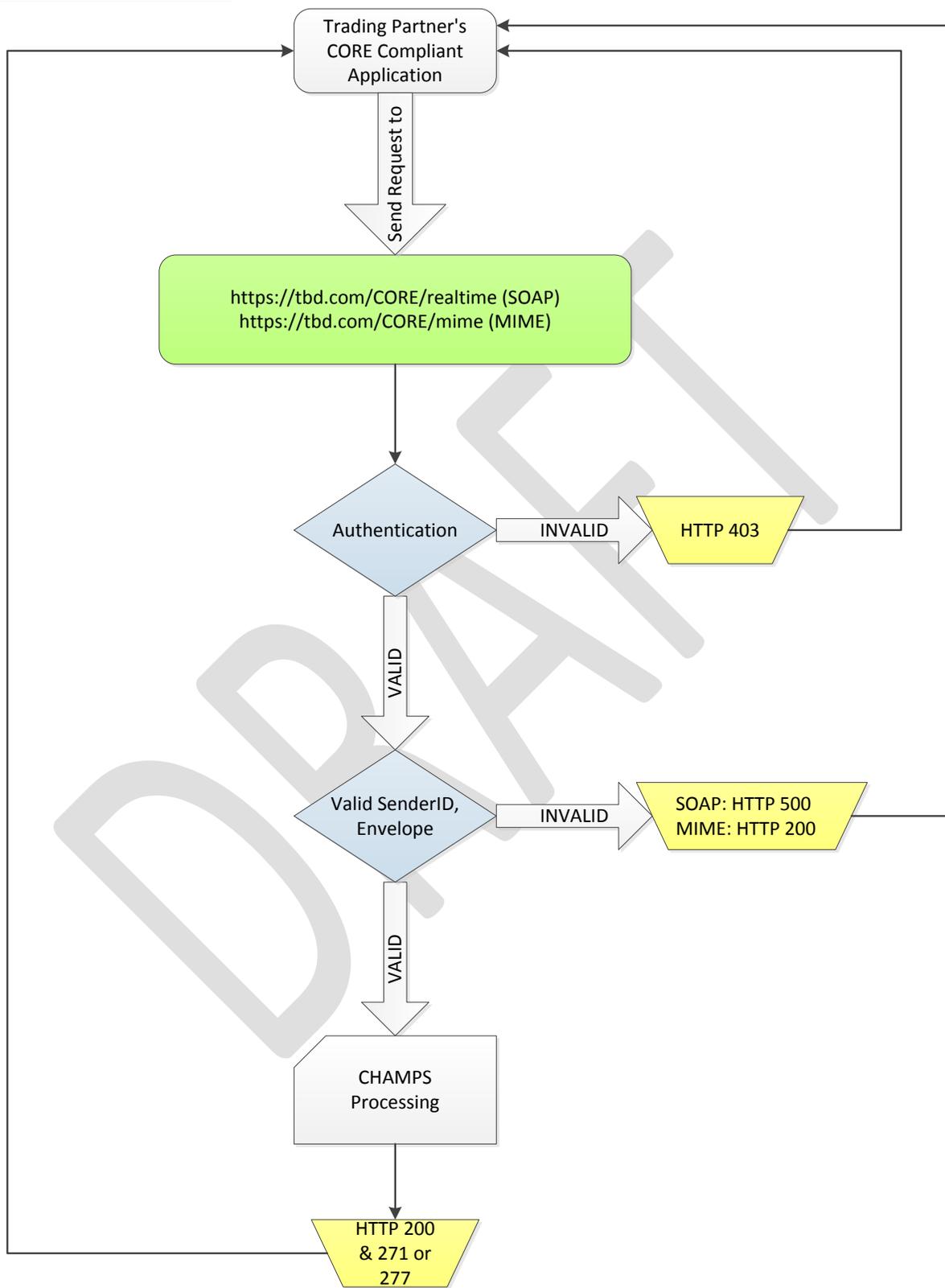
6.3.1 Real-time Request and Response Handling

HTTP/S supports a request-response message pattern, meaning that the sender submits a message and then waits for a response from the message receiver. The process for real-time request and response works as follows.

1. The user application submits a real-time SOAP or MIME request.
 - a. Submit SOAP to <URL to be published>
Real Time:
Production: TBD
Testing: <https://corevertimeqa.state.mi.us/ecams/soap?wsdl>
Batch:
Production: TBD
Testing: <https://corebatchqa.state.mi.us/ecams/soap?wsdl>
 - b. Submit MIME to <URL to be published>
Real Time:
Production: TBD
Testing: <https://corevertimeqa.state.mi.us/ecams/multipart>
Batch:
Production: TBD
Testing: <https://corebatchqa.state.mi.us/ecams/multipart>
 - c. Testing: <https://corebatchqa.state.mi.us/ecams/multipart>
2. The CHAMPS system authenticates the username and password. If unable to authenticate, an HTTP 403 Forbidden response is returned.
3. If the username and password are successfully authenticated, an HTTP 200 OK status response is returned to the user within 20 seconds along with the 271 or 277 response.
4. The CHAMPS system validates SenderId and other elements of the CORE envelope metadata. If validation fails, the following errors are returned:
 - a. For SOAP: HTTP 500 SOAP fault with Code=Sender & Reason=Authentication Failure
 - b. For MIME: HTTP 200 with ErrorCode=Sender & ErrorMessage=Authentication Failure

The diagram below depicts the real-time request and response flow.

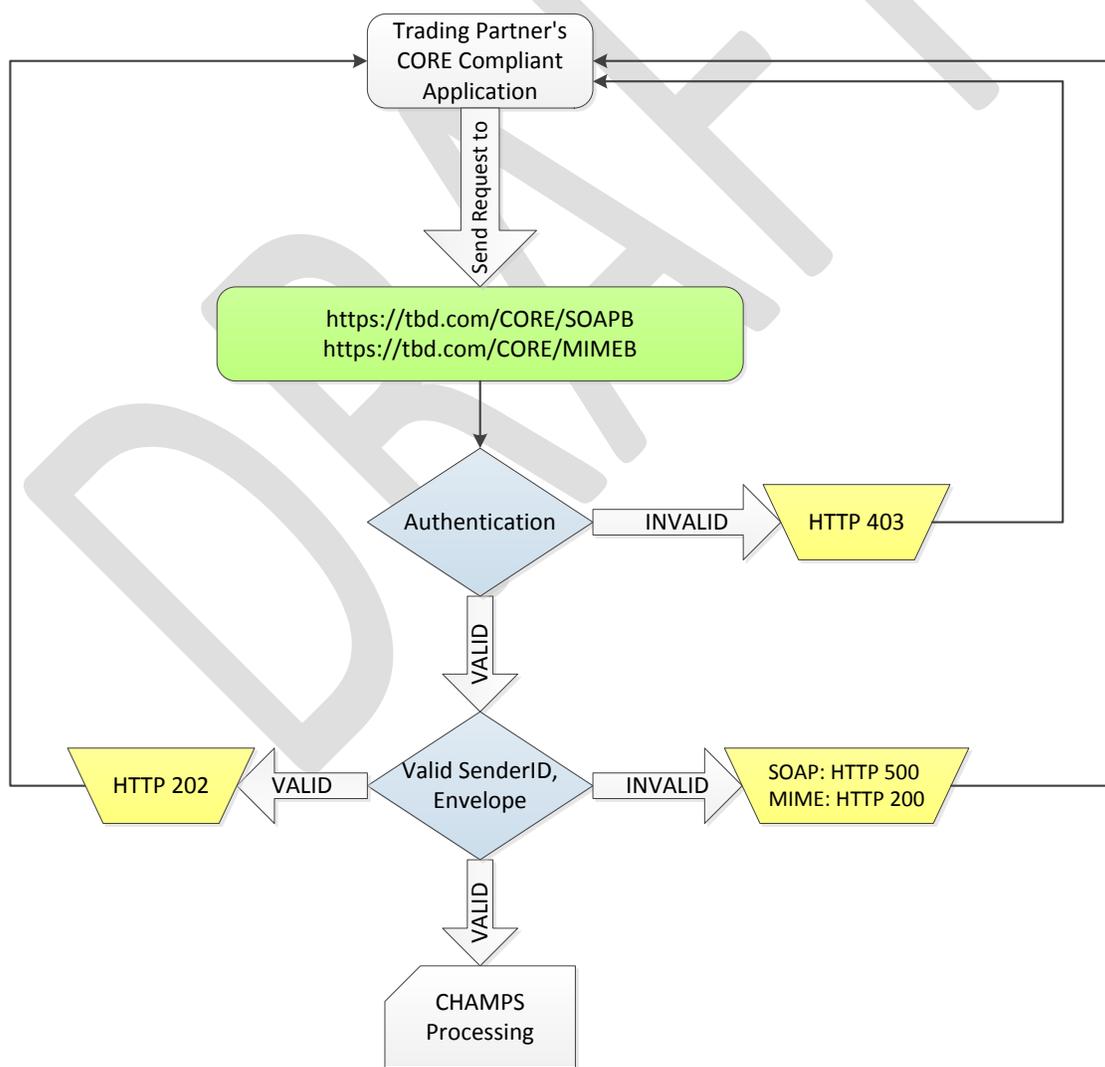
Real-time Process Flow



6.3.2 Batch Request and Response Handling

Initial Batch Submission

1. The user application submits a batch SOAP or MIME request.
 - a. Submit SOAP to <URL to be published>
 - b. Submit MIME to <URL to be published>
2. The CHAMPS system authenticates the username and password. If unable to authenticate, an HTTP 403 Forbidden response is returned.
3. The CHAMPS system validates SenderId and other elements of the CORE envelope metadata. If validation fails, the following errors are returned:
 - a. For SOAP: HTTP 500 SOAP fault with Code=Sender & Reason=Authentication Failure
 - b. For MIME: HTTP 200 with ErrorCode=Sender & ErrorMessage=Authentication Failure
4. If the username and password are successfully authenticated and the envelope metadata validated, an HTTP 202 OK status response is returned to the user indicating CHAMPS has accepted the batch submission for processing.

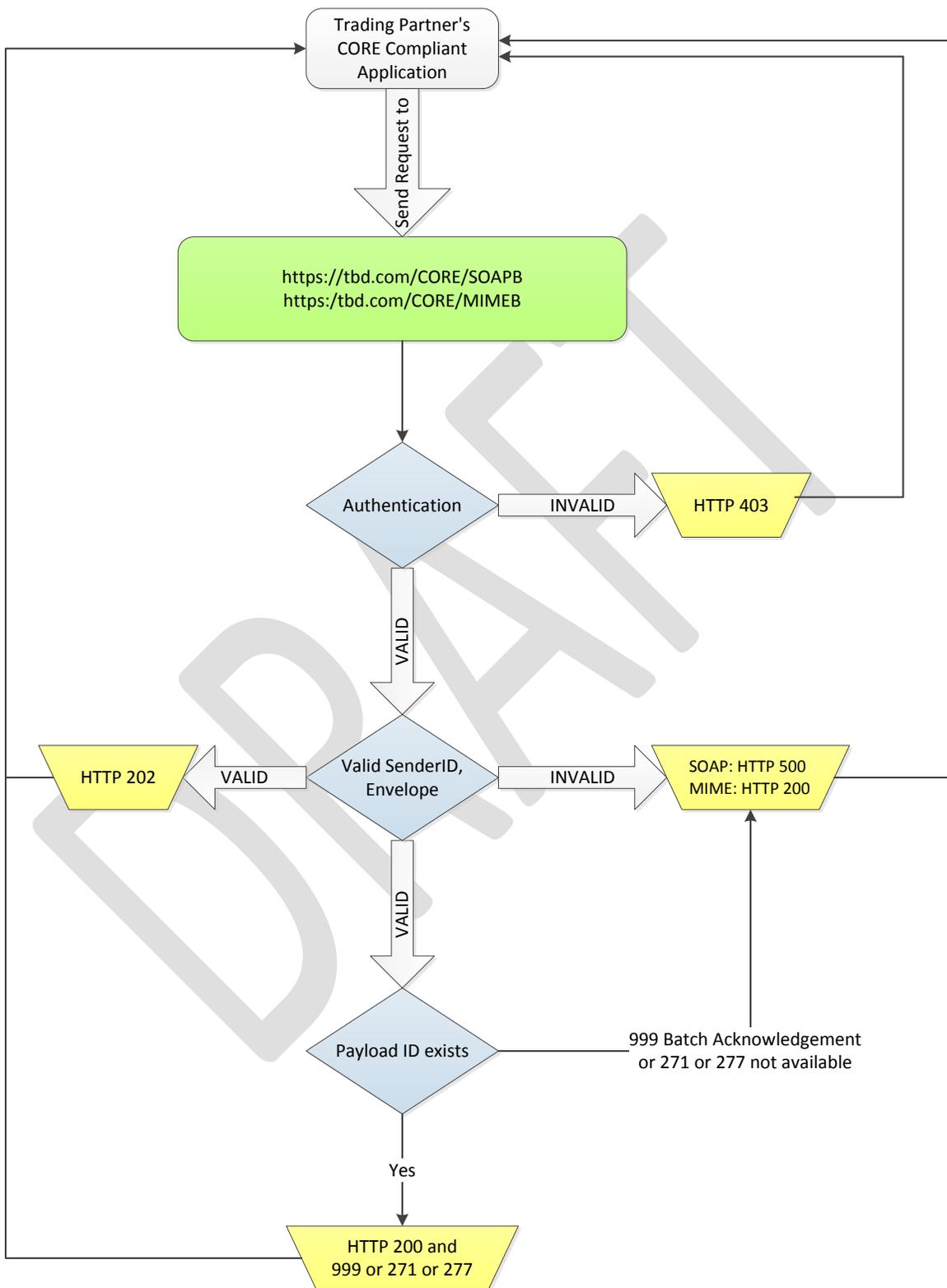


Batch Pickup

1. The user application submits a time-delayed batch pickup request.
 - a. Submit SOAP to <URL to be published>
 - b. Submit MIME to <URL to be published>
2. The CHAMPS system authenticates the username and password. If unable to authenticate, an HTTP 403 Forbidden response is returned.
3. The CHAMPS system validates SenderId and other elements of the CORE envelope metadata. If validation fails, the following errors are returned:
 - a. For SOAP: HTTP 500 SOAP fault with Code=Sender & Reason=Authentication Failure
 - b. For MIME: HTTP 200 with ErrorCode=Sender & ErrorMessage=Authentication Failure
4. If the username and password are successfully authenticated and the envelope metadata validated, an HTTP 202 response is sent and a match for PayloadID will be performed for an acknowledgement or response transaction, as appropriate for Payload Type. If no match occurs, an HTTP 400 status response is returned.
5. If a PayloadID match occurs, one of the following will be generated back to the user with an HTTP 200 status.
 - a. A 999 Reject response will be available within one hour if there is a problem with the segments occurring between the ISA and IEA.
 - b. A 999 Acceptance response will be available within one hour if no problems are found.
 - c. When the 270 or 276 transaction is submitted by 9pm on a business day, the 271 or 277 response transaction will be available by 7am the next business day.
Note: Multiple interchanges may be returned within the same Payload.

The diagram on the next page depicts the Batch Pickup flow.

Batch Pickup Process Flow



6.4 Transmission Administrative Procedures

Response Times: A response to the real-time inquiry will be provided within 20 seconds during hours of availability. A response to a batch inquiry submitted by 9:00 p.m. on a business day will be provided by 7:00 a.m. the following business day.

6.5 Retransmission Procedures

If a real-time response message is not received within the 60-second response period, the submitter's system should send a duplicate transaction no sooner than 90 seconds after the original attempt was sent.

If no real-time response is received after the second attempt, the submitter's system should submit no more than 5 duplicate transactions within the next 15 minutes. If the additional attempt results in the same timeout termination, the submitter's system should notify the submitter to contact MDCH directly to determine if system availability problems exist or if there are known internet traffic constraints causing the delay. Please verify the file contents before any further resubmission.

6.6 Communication Protocols

6.6.1 HTTP MIME Multipart

MDCH supports standard HTTP MIME messages. The MIME format used must be that of multipart/form-data. Responses to transactions sent in this manner will also be returned as multipart/form-data.

6.6.2 SOAP + WSDL

MDCH also supports transactions formatted according to the Simple Object Access Protocol (SOAP) conforming to standards set for the Web Services Description Language (WSDL) for XML envelope formatting, submission, and retrieval.

- SOAP XML Schema
The XML schema definition set forth by CORE is located at:
<http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd>
- WSDL Information
The WSDL definition set forth by CORE is located at:
<http://www.caqh.org/SOAP/WSDL/CORERule2.2.0.xsd>

6.6.3 Header Requirements

The envelope metadata requirements are described briefly in the table below.

Field	Accepted Values	Comment
PayloadType	X12_270_Request_005010X279A1 X12_005010_Request_Batch_Results_271 X12_276_Request_005010X212 X12_005010_Request_Batch_Results_277 X12_TA1_Response_00501X231A1 X12_999_Response_005010X231A1	Real-time & batch submissions Batch results retrieval for 270/271 Real-time & batch submissions Batch results retrieval for 276/277 TA1 response (real-time) 999 response (real-time)
ProcessingMode	RealTime Batch	Batch used for either submission or pickup
PayloadID	PayloadID will conform to ISO UUID standards (described at ftp://ftp.rfceditor.org/in-notes/rfc4122.txt), with hexadecimal notation, generated using a combination of local timestamp (in milliseconds) as well as the hardware (MAC) address33, to ensure uniqueness.	
Payload Length	Length of the X12 document	Required only if ProcessingMode is Batch; otherwise do not send.
TimeStamp	YYYY-MM-DDTHH:MM:SSZ	See http://www.w3.org/TR/xmlschema11-2/#dateTime
User Name	MDCH Assigned	For SOAP+WSDL and MIME Multipart use only.
Password	MDCH Assigned	For SOAP+WSDL and MIME Multipart use only.
SenderID	MDCH Assigned	This is assigned based on how you are enrolled in CHAMPS. It will be your NPI number, Provider ID, or DEG ID.

Field	Accepted Values	Comment
ReceiverID	D00111	This is the Michigan Medicaid receiver ID.
CORERuleVersion	2.2.0	
Checksum	Checksum of the X12 document	Algorithm is SHA-1; encoding is Hex; required only if ProcessingMode is Batch. Checksum must be computed only on the payload and not on the metadata. Do not send for Real-time.
Payload		Contains the X12 request.

6.6.4 Error Reporting

The HTTP and envelope processing status and error codes are described briefly here. For comprehensive instructions on using the SOAP+WSDL and MIME Multipart transport protocols, please use the web references provided earlier in this section in addition to the information provided here.

HTTP Status and Error Codes

The HTTP status and error codes included in the following table represent only a few of the commonly used status and error codes in the standard. An exhaustive list of HTTP Status Codes and descriptions are included in the HTTP specification at:

<http://tools.ietf.org/html/rfc2616#section-6.1.1>

HTTP Status/Error Codes (Normative, Not Comprehensive)	Status Code Description (Intended Use)
200 OK	Success
202 Accepted	Batch file submission has been accepted (but not necessarily processed)
400 Bad Request	Incorrectly formatted HTTP headers
403 Forbidden	Access denied
500 Internal Server Error	The web-server encountered a processing error, or there was a SOAP fault (in case of SOAP envelope method)
5xx Server errors	Standard set of server side errors (e.g. 503 Service Unavailable)

Envelope Processing Status and Error Codes

When SOAP is used, some of the CORE-compliant Envelope Processing errors map to SOAP faults (see <http://www.w3.org/TR/soap12-part1/#soapfault>). To handle CORE-compliant envelope processing status and error codes, two fields called ErrorCode and ErrorMessage are included in the CORE-compliant Envelope. ErrorMessage is a free form text field that describes the error (for the purpose of troubleshooting and logging). When an error occurs, PayloadType is set to CoreEnvelopeError.

The following table shows commonly used error codes and descriptions.



CORE-compliant Envelope Processing Status/Error Codes (Normative, Comprehensive)	Status Code Description (Intended Use)
Success	Envelope was processed successfully.
<FieldName>Illegal	Illegal value provided for <FieldName>.
<FieldName>Required	The field <FieldName> is required but was not provided.
<FieldName>NotUnderstood	The field <FieldName> is not understood at the receiver. In the case of SOAP, this error is returned as a NotUnderstood SOAP fault.
VersionMismatch	The version of the envelope sent is not acceptable to the receiver. If the SOAP version is not valid at the receiver, a SOAP fault is returned with this fault code.
Unauthorized	The username/password or Client certificate could not be verified.
ChecksumMismatched	The checksum value computed on the recipient did not match the value that was sent in the envelope.
Sender	The envelope sent by the sender did not conform to the expected format. In the case of SOAP, this error should be sent as a SOAP fault with "Sender" fault code.
Receiver	The message could not be processed for reasons attributable to the Receiver (e.g., upstream process is not reachable). In the case of SOAP, this error should be sent as a SOAP fault with "Receiver" fault code.

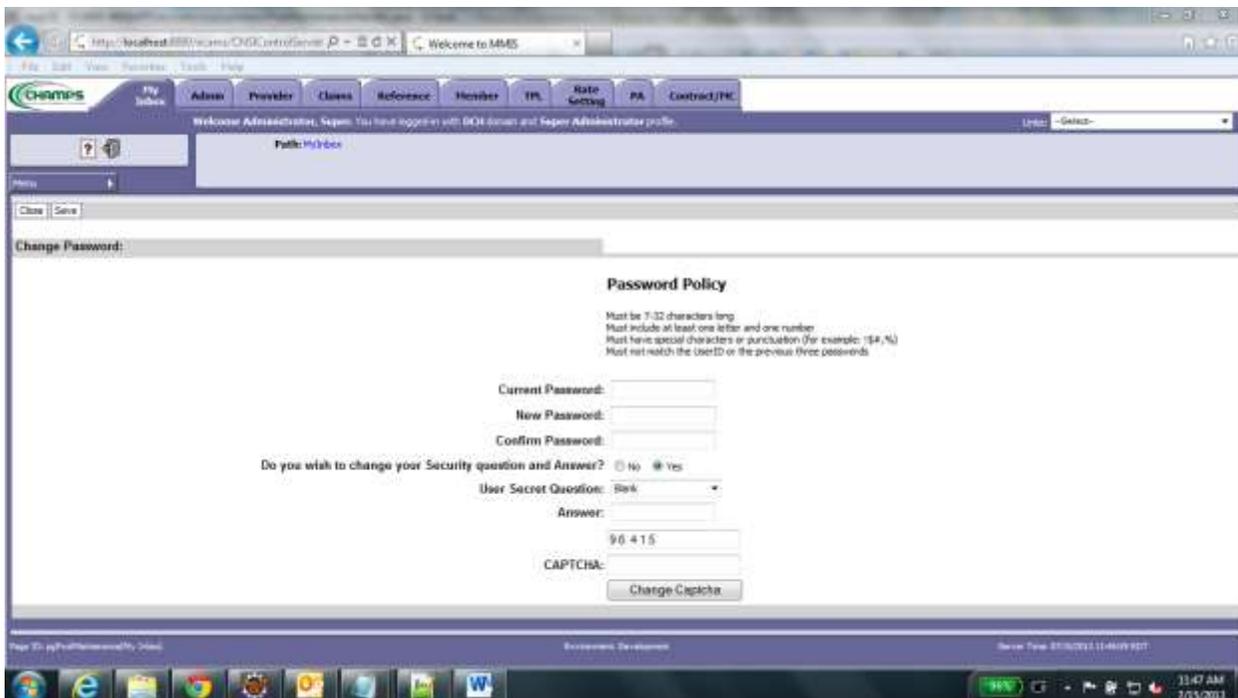
6.7 Passwords

A username and password is required to authenticate the submitted transaction request when using the SOAP+WSDL or MIME Multipart modes.

- ❖ Providers can contact Automated Billing at automatedbilling@michigan.gov (please use a subject line of "CORE Password Request") to request a username and password for use with SOAP+WSDL or MIME Multipart modes.
- ❖ Providers can reset their password using CHAMPS password maintenance screens. Please note, anyone with a Domain Administrator role has the authority to update passwords for your organization.

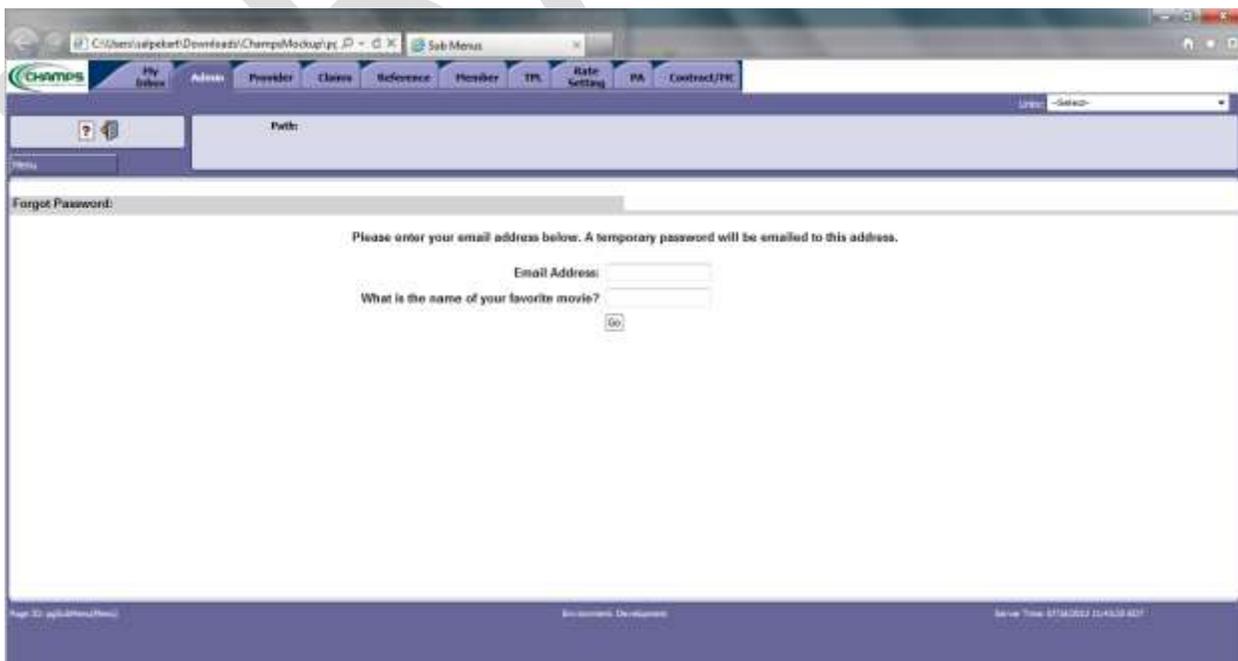
Password Maintenance

To change your password, log into CHAMPS and select the My Inbox tab, navigate to the "EDI Password Maintenance" screen (shown below), and enter the requested information. Passwords must be changed every 120 days.



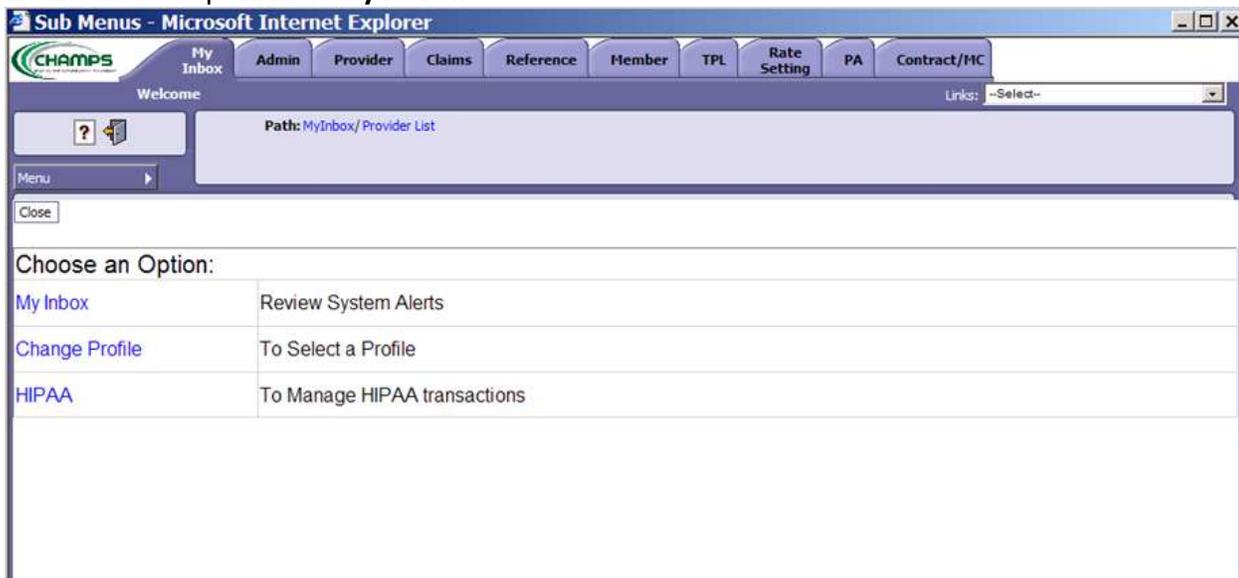
Password Recovery

To recover a lost password, log into CHAMPS, select the My Inbox tab, navigate to the “EDI Password Recovery” screen (shown below), and enter the required data. A temporary password is emailed to the email address provided on the screen if the security question is correctly answered.

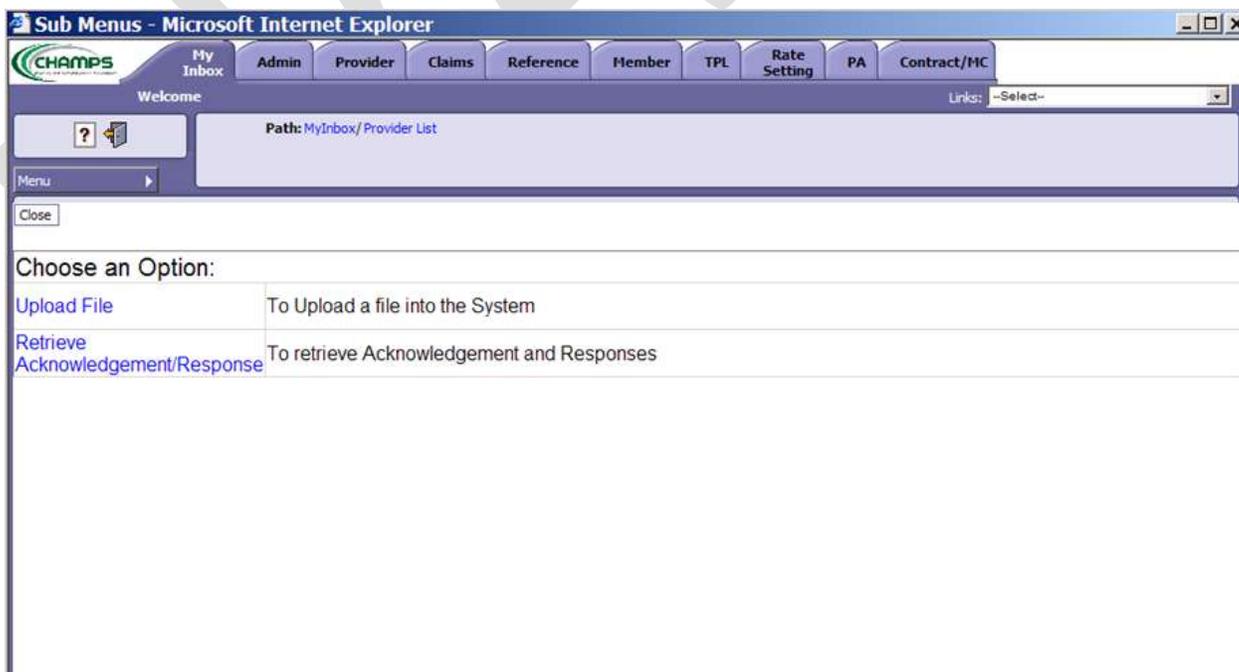


Section 7 - ELECTRONIC BATCH WEB UPLOAD THROUGH CHAMPS

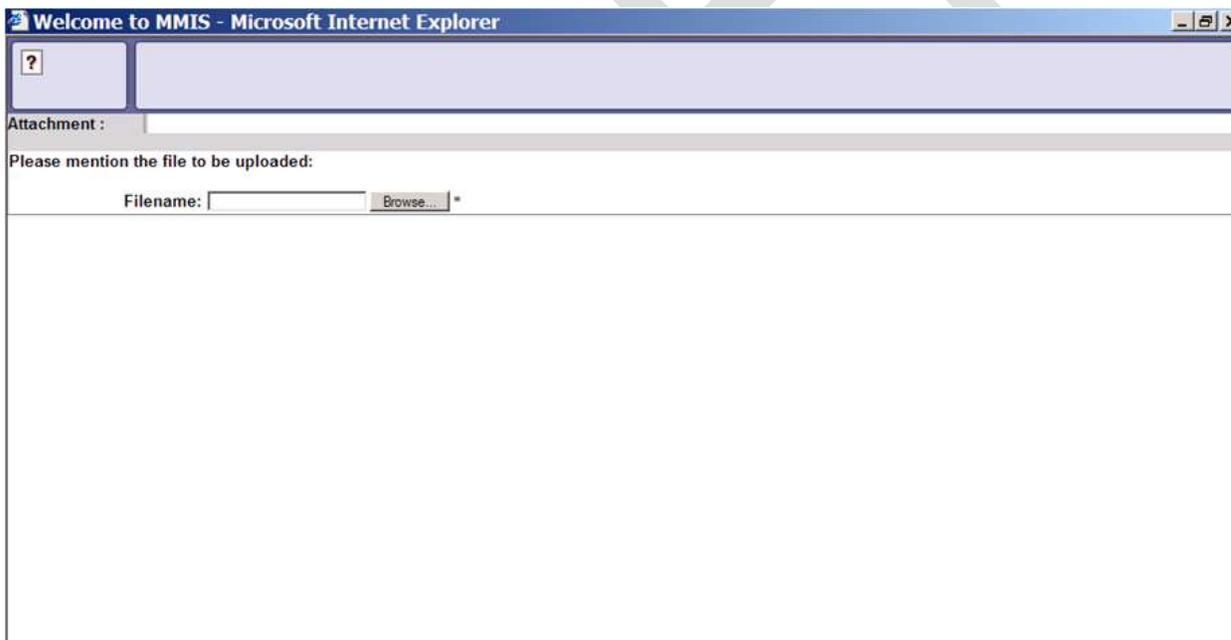
1. Log on as a billing agent or NPI. If using Billing Agent or NPI the enrollment must have Electronic Batch in their mode of claim submission.
2. Need either CHAMPS full access or Billing Agent Access
3. From tabs at the top click on **My In Box**



4. Click on **HIPAA**



5. Click on **Upload File**



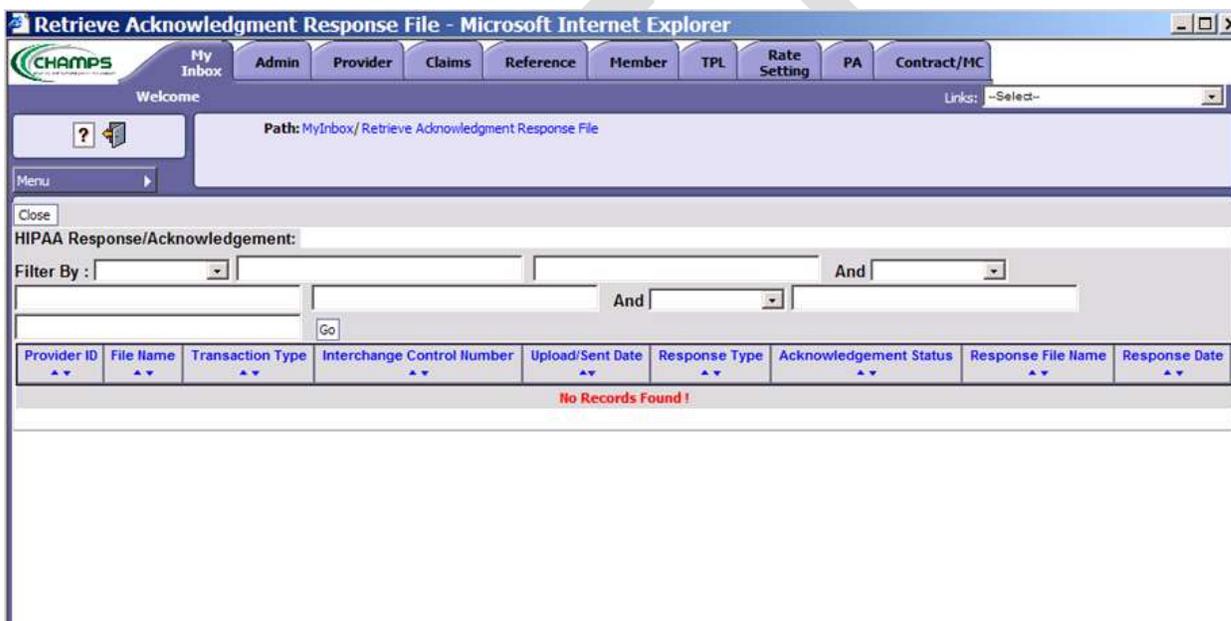
Please note:

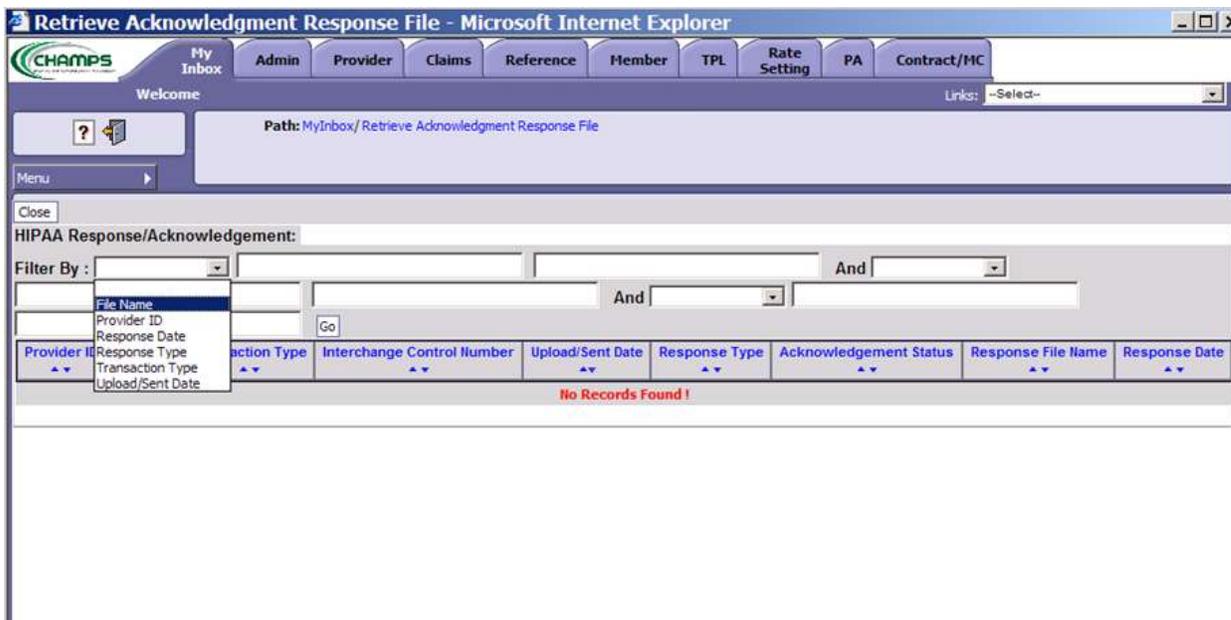
1. The file name must include the Application ID from the list below.
 - 5475(837) – Health Care Claim
 - 5414(270) – Eligibility Inquiry
 - 4952(276) – Claim Status Inquiry
 - 5386(278) – Prior Authorization Inquiry
2. A new file-naming convention was implemented for all Electronic Web upload files. The following examples are based on how you log into CHAMPS by NPI or Provider ID.

- NPI.5475.CCYMMDDhhmm
(example: 1234567890.5475.201210261208.dat)
 - ProviderID.5475.CCYMMDDhhmm
(example: 1234567.5475.201210261209.dat)
3. All web batch files must have an extension of .dat.
 4. A file size of 50kb file or smaller is acceptable.
 5. You can send in as many files as you want per day.

Retrieving Files

1. Within 1 hour you should logon to CHAMPS and go back in to:
 - My In box
 - HIPAA
2. Retrieve acknowledgement/response and download your 999.





3. File Name is used most often: %00??% (for DEG ID) %NPI% (for Provider Billing NPI 10 digits) or %Champs ID% (7 digit Provider ID). This is depending on how you logged into Champs submit your file= Deg ID or NPI or Provider ID.
4. Review your acknowledgement to make sure your file was accepted

Section 8 - B2B TESTING

Business to Business (B2B) testing is the process of submitting test files to MDCH for validation. This section describes B2B testing for HIPAA v5010 transactions.

MDCH has two-stages of testing process for Trading Partners. Only HIPAA 5010 files will be accepted.

Billing Agent IDs for New Trading Partners

New Trading Partners (who do not already have a billing agent ID with MDCH) will need to apply for a Billing Agent ID. For more information please refer to www.michigan.gov/MDCH > Providers > Trading Partners > How to Become an e-Biller.

5010 Test Instructions by Transaction

For specifics on testing and the v5010 certification criteria, please review the B2B Testing Instructions posted at www.michigan.gov/tradingpartners. The summary below will give you an overview of the testing process.

Stage 1 - Integrity Testing (open for all Trading Partners)

Integrity testing is required for all electronic submitters and must be completed before a Trading Partner can start Stage 2 testing, using the *EDIFECs* Ramp Manager automated testing website. Ramp Manager is an easy-to-use environment to test v5010 transactions for syntax errors, and is available at no cost to MDCH's Trading Partners. More information on integrity testing is available at www.michigan.gov/tradingpartners. Once you have submitted a test file for Stage 1 send an e-mail: automatedbilling@michigan.gov)

Stage 2 – CHAMPS B2B Testing (Available after passing Stage 1 testing thru Ramp Manager and is available to all Trading Partners).

For Stage 2 testing, you must successfully complete Stage 1 testing. Refer to “Billing Agent IDs for New Trading Partners” above for instructions on how to become a Billing Agent in CHAMPS and “5010 Test Instructions by Transaction” above for instructions on creating test files. Please refer to the following sections in this manual regarding file submission and file naming conventions:

DATA EXCHANGE GATEWAY (DEG) Section 4 Pg. 7

SSLFTP/SFTP (WS_FTP) SETUP FOR THE DEG Section 5.2 Pg. 24

ACA CORE TRANSPORT MODES Section 6.3.1 Pg. 39

ELECTRONIC BATCH WEB UPLOAD THROUGH CHAMPS Section 7 Pg. 50

APPLICATION ID/FILENAME Section 10 Pg. 61

Once a test file is submitted to the DEG, you must send an email, including a contact name, telephone number, and email in your organization, to Automated Billing at automatedbilling@michigan.gov to inform MDCH that a test file has been submitted.

Electronic Submissions Manual

To ensure proper retrieval of your files, please use a subject line in your email of: "5475T or 5476T Test File DCH00??"; where DCH00?? is your Billing Agent ID.

(For example: "5475T Test File DCH00??")

Your files will be retrieved and processed thru the Testing System. We will not send you a TA1 or 999 Acknowledgment back on these files until they have been uploaded to the test environment. Once that is done, you can retrieve your TA1 or 999 in your DEG mailbox.

If you have questions, please contact Automated Billing at automatedbilling@michigan.gov.

DRAFT

Section 9 - 999 Acknowledgement File

The 999 acknowledgement file is a document that billing agents can use to verify that the files they submitted were received by MDCH. MDCH requests that all billing agents save all acknowledgement files until claims appear on a Remittance Advice (RA). This will show proof of receipt that the files were submitted to MDCH.

Below is an example of an Accepted 999, please note that certain areas are marked out due HIPAA regulations.

```
ISA*00*      *00*      *ZZ*D00111      *ZZ*00??  
*120425*1551*^*00501*000000001*0*P*:~  
  
GS*FA*D00111*00??*20120425*1551*1*X*005010X231~  
ST*999*0001*005010X231~  
AK1*HC*95*005010X223A2~  
AK2*837*000000220*005010X223A2~  
IK5*A~  
AK2*837*000000221*005010X223A2~  
IK5*A~  
AK2*837*000000222*005010X223A2~  
IK5*A~  
AK2*837*000000223*005010X223A2~  
IK5*A~  
AK2*837*000000224*005010X223A2~  
IK5*A~  
AK9*A*5*5*5~  
SE*14*0001~  
GE*1*1~  
IEA*1*000000001~
```

Electronic Submissions Manual

Below is an example of an Accepted 999 with non-fatal errors and was accepted for further processing. Each error is identified in the IK3 and IK4 segments. Please refer to the HIPAA TR3 guideline or Michigan Companion Guide.

ISA*00* *00* *ZZ*D00111 *ZZ*00??
*120426*1701*^*00501*000000001*0*P*:~

GS*FA*D00111*00??*20120426*1701*1*X*005010X231~
ST*999*0001*005010X231~

AK1*HC*126*005010X222A1~

AK2*837*000020606*005010X222A1~

IK5*A~

AK2*837*000020637*005010X222A1~

IK3*HI*3952*2300*8~

CTX*CLM01:0014887951~

IK4*1:2*1271*I12*E8889~

IK5*E*I5~

AK2*837*000020650*005010X222A1~

IK5*A~

AK9*E*3*3*3~

SE*13*0001~

GE*1*1~

IEA*1*000000001~

Below is an example of a Partially Accepted 999 with fatal and non-fatal errors for further processing. Each error is identified in the IK3 and IK4 segments. Keep in mind you can have the same fatal or non-fatal error multiple times throughout the file. Please refer to the HIPAA TR3 guideline or Michigan Companion Guide.

ISA*00* *00* *ZZ*D00111 *ZZ*00??
*120426*1540*^*00501*000000001*0*P*:~

GS*FA*D00111*00??*20120426*1540*1*X*005010X231~

ST*999*0001*005010X231~

AK1*HC*126*005010X222A1~

AK2*837*000020575*005010X222A1~

IK5*A~

AK2*837*000020576*005010X222A1~

IK5*A~

AK2*837*000020577*005010X222A1~

IK3*SVD*3619*2430*8~

CTX*CLM01:TPRF1106003808401~

IK4*3:5*1339*I13*KX~

CTX*SITUATIONAL TRIGGER*SVD*3619**3:4*3:1339~

IK5*R*5*I5~

AK2*837*000020578*005010X222A1~

IK3*HI*3952*2300*8~

CTX*CLM01:0014887951~

IK4*1:2*1271*I12*E8889~

IK3*REF*4494*2400*8~

CTX*CLM01:0014831301~

IK4*2*127*I12*23D01025908~

IK3*REF*4522*2400*8~

CTX*CLM01:0014831301~

IK4*2*127*I12*23D01025908~

IK3*REF*4546*2400*8~

CTX*CLM01:0005893440~

Electronic Submissions Manual

IK4*2*127*112*23D01025908~
IK3*REF*4570*2400*8~
CTX*CLM01:0005893440~
IK4*2*127*112*23D01025908~
IK3*REF*4617*2400*8~
CTX*CLM01:0013800419~
IK4*2*127*112*23D01025908~
IK3*REF*4645*2400*8~
CTX*CLM01:0013822403~
IK4*2*127*112*23D01025908~
IK3*REF*4673*2400*8~
CTX*CLM01:0014902207~
IK4*2*127*112*23D01025908~
IK3*REF*4697*2400*8~
CTX*CLM01:0014894637~
IK4*2*127*112*23D01025908~
IK5*R*5*I5~
AK2*837*000020579*005010X222A1~
IK3*AMT*116*2320*8~
CTX*CLM01:BA-108989T37863~
IK4*2*782*112*-6.07~
IK3*SVD*128*2430*8~
CTX*CLM01:BA-108989T37863~
IK4*2*782*112*-6.07~
IK5*R*5*I5~
AK2*837*000020580*005010X222A1~
IK5*A~
AK2*837*000020581*005010X222A1~
IK3*NM1*43*2310*8~
CTX*CLM01:CLM49978~

IK4*4*1036*19~

IK3*NM1*74*2310*8~

CTX*CLM01:CLM50836~

IK4*4*1036*19~

IK5*E*15~

AK2*837*000020582*005010X222A1~

IK3*SV1*17823*2400*8~

CTX*CLM01:4759~

IK4*2*782*I12*5~

CTX*SITUATIONAL TRIGGER*SV1*17823**1:2*3:234~

IK5*E*15~

AK2*837*000020583*005010X222A1~

IK5*A~

AK2*837*000020584*005010X222A1~

IK3*SV1*60*2400*8~

CTX*CLM01:M1182931T22430~

IK4*2*782*I12*.1~

CTX*SITUATIONAL TRIGGER*SV1*60**1:2*3:234~

IK5*E*15~

AK2*837*000020585*005010X222A1~

IK5*A~

AK9*P*11*11*8~ notice the count changed to reflect 3 transactions that have failed.

SE*921*0001~

GE*1*1~

IEA*1*000000001~

From the example above, the IK3 segment verifies the segment Position of segment within Transaction Set (120) and Segment Has Data Element Errors Qualifier (8).

The IK4 segment gives you the Data Element Position within the Segment (2), the X12 Data Dictionary Reference ID (782), Segment has Data Element Errors (I12), and a Copy of Data Element in Error (92.511)

Section 10 - APPLICATION ID/FILENAME

You will need to use the 'Application ID File Name' for files that are submitted through the DEG to MDCH, and to recognize files that MDCH returns to your billing agent "mailbox". If you submit a file that is not listed, please contact AutomatedBilling@michigan.gov for more information.

Application ID Filename*	Transaction ID	Transaction Information
5414	270	Medical Eligibility Inquiry
5415	271	Medical Eligibility Response
4952	276	Health Care Claim Status Inquiry
4953	277	Health Care Claim Status Response
5386	278	Prior Authorization Request
5383	278	Prior Authorization Response
4987	835	Health Care Payment and RA
5475	837	FFS Health Care Claims
5475T	837	FFS Health Care TEST Claims
5476	837	Encounters Claims (v5010)
5476T	837	Encounters TEST Claims
5477		NCPDP Claims
5477T		NCPDP TEST Claims

***Note:** A "T" must be placed in the fifth position of the Application ID Filename to identify a test file.