Table of Contents

Section 1 - INTRODUCTION ............................................................................................................. 4
  1.1 Medicaid Billing Agents .................................................................................................................. 4
Section 2 - RESOURCES .................................................................................................................... 5
Section 3 - SOFTWARE AND PROGRAMMING ........................................................................... 6
Section 4 - FILE TRANSFER SERVICE (FTS) [former name: DEG] ....................................... 7
  4.1 FTS - Internet Connection ............................................................................................................. 7
    4.1.1 Java and Non-Java Mode .......................................................................................................... 7
    4.1.2 PC Setup .................................................................................................................................. 7
    4.1.3 Logging onto the MDHHS Internet Connection ................................................................. 8
    4.1.4 Downloading Files from FTS ................................................................................................. 9
    4.1.5 Uploading Files to the FTS ..................................................................................................... 10
Section 5 - SSLFTP/SFTP (WS_FTP) SETUP FOR THE FTS .................................................. 14
  5.1 Overview ..................................................................................................................................... 14
  5.2 WS_FTP Pro Version 2007 .......................................................................................................... 14
    5.2.1 Main WS_FTP Screen (WS_FTP Professional Version 2007) ........................................ 14
    5.2.2 Options Menu > Program Options (Program Options Version 2007) ..................... 15
    5.2.3 Example of Site Setup for SSLFTP WS_FTP Professional Version 2007 ................ 17
    5.2.4 Example of Site Setup for SFTP (WS_FTP Professional Version 7) ......................... 20
    5.2.5 Certificate Screen (Version 2007) ....................................................................................... 23
    5.2.6 Example of Good Transfer Log ............................................................................................ 23
  5.3 Connecting Issues ....................................................................................................................... 25
  5.4 Change File Directories .............................................................................................................. 25
Section 6 - ACA CORE TRANSPORT MODES ............................................................................. 27
  6.1 Connectivity Overview ................................................................................................................. 27
  6.2 System Availability ...................................................................................................................... 28
    6.2.1 Real-time Inquiry Response .................................................................................................. 28
    6.2.2 Batch Inquiry Response ....................................................................................................... 28
  6.3 Process Flows ............................................................................................................................... 28
    6.3.1 Real-time Request and Response Handling ........................................................................ 28
    6.3.2 Batch Request and Response Handling ............................................................................. 30
  6.4 Transmission Administrative Procedures ................................................................................... 34
6.5 Retransmission Procedures........................................................................................................34
6.6 Communication Protocols........................................................................................................34
  6.6.1 HTTP MIME Multipart .......................................................................................................34
  6.6.2 SOAP + WSDL ..................................................................................................................34
  6.6.3 Header Requirements ........................................................................................................35
  6.6.4 Error Reporting ..................................................................................................................36
Section 7 - PASSWORDS ..................................................................................................................37
  7.1 SOAP+WSDL and MIME Multipart Passwords .................................................................37
    7.1.1 Password Maintenance ....................................................................................................38
    7.1.2 Password Replacement ..................................................................................................39
  7.2 SSLFTP/SFTP Passwords .......................................................................................................39
  7.3 File Transfer Service (FTS) Passwords ..................................................................................40
    7.3.1 Change Password function ............................................................................................40
    7.3.2 Unknown Password ........................................................................................................40
Section 8 - ELECTRONIC BATCH WEB UPLOAD THROUGH CHAMPS .............................................40
Section 9 - B2B TESTING ..................................................................................................................44
  9.1 Billing Agent IDs for New Trading Partners ...........................................................................44
  9.2 5010 Test Instructions by Transaction ..................................................................................44
  9.3 Stage 1 - Ramp Manager Testing ..........................................................................................44
  9.4 Stage 2 - CHAMPS B2B Testing ............................................................................................44
Section 10 - 999 ACKNOWLEDGEMENT FILE ............................................................................45
Section 11 - CLASS ID/FILENAME (formerly, ‘Appl ID Filename’) .................................................50
  11.1 *Notes Regarding TEST Files ............................................................................................51
Section 1 - INTRODUCTION

Michigan’s data-submission portal is the File Transfer Service (FTS); however, it has previously been referred to as the Data Exchange Gateway, or DEG. Some documents may still reference the Data Exchange Gateway (DEG); be aware that a reference to the DEG portal is a reference to the FTS. Refer to Section 4 for further information.

This Electronic Submission Manual (ESM) describes how to submit data electronically to the Michigan Department of Health and Human Services (MDHHS). Section 4, File Transfer Service (FTS), explains how to communicate with MDHHS through an Internet connection, SSLFTP connection, or using the ACA CORE required SOAP+WSDL or HTTP/S MIME transport modes.

Instructions are also included 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 exchange Medicaid transactions or queries, you must first test your electronic transactions with MDHHS to insure adherence with national and Michigan standards, and to reduce errors in your production file submissions to MDHHS.

This document replaces all previous MDHHS Electronic Submission Manuals.

1.1 Medicaid Billing Agents

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 refer to the Resources in the following 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 provides the necessary instructions for the actual transmission and receipt of electronic information. Only billing agents will be able to send and retrieve information with MDHHS.

Any entity submitting a 270 eligibility or a 276 claim status request must first be associated in CHAMPS with the Billing Agent or Trading Partner that originated the claim.
**Section 2 - RESOURCES**

MDHHS informational resources for electronic billing can be found at the MDHHS website:


Please make sure to review the documentation available at the website before contacting MDHHS directly. This ESM and other resources are available at the MDHHS website, including:

- CHAMPS Testing Instructions for 837 Fee for Service (FFS) Claims, 837 Encounters, NCPDP files, and 270, 276, and 278 Requests
- Electronic Updates
- Michigan Companion Guides
- 835 Electronic Remittance Advice Instructions
- Links to additional Information about electronic Health Care transactions

Michigan’s *EDI Services, B2B Testing, Provider Support* and *Encounter* teams are available to assist you:

<table>
<thead>
<tr>
<th>EDI Services -</th>
<th>Michigan Medicaid’s EDI Services Unit will handle all questions related to electronic Fee For Service (FFS) claims file exchange and FTS issues.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website:</td>
<td><a href="http://michigan.gov/tradingpartners">http://michigan.gov/tradingpartners</a></td>
</tr>
<tr>
<td>EDI Services Email:</td>
<td><a href="mailto:AutomatedBilling@michigan.gov">AutomatedBilling@michigan.gov</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business to Business (B2B) Testing -</th>
<th>The B2B Test Team will handle test processing of electronic transactions. Trading Partners (including new Providers, Billing Agents, Clearinghouses, and Health Plans) are required to initially test prior to sending electronic transactions. Michigan provides two test systems for this purpose: <em>Ramp Manager</em> (format and syntax testing) and <em>CHAMPS B2B</em> (claim adjudication testing). Please access the MDHHS website for testing information, and contact <em>EDI Services</em> or the <em>B2B Test Team</em> to obtain test system access credentials and further instructions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2B Testing Email:</td>
<td><a href="mailto:MDHHS-B2B-Testing@michigan.gov">MDHHS-B2B-Testing@michigan.gov</a></td>
</tr>
</tbody>
</table>
### Provider Support Unit

The Provider Support Unit will handle all billing questions.

**Website:** [http://michigan.gov/mdhhs](http://michigan.gov/mdhhs) >> Doing Business with MDHHS >> Health Care Providers >> Providers >> CHAMPS

**Provider Support Line:** 1-800-292-2550

**Provider Support Email:** ProviderSupport@michigan.gov

### Encounter Team

The Encounter Team will handle all electronic questions related to Encounter file submission and FTS issues for Trading Partners. The Encounter team also handles issues related to NCPDP submissions.

**Encounter Support Email:** MDHSEncounterData@michigan.gov

### Section 3 - SOFTWARE AND PROGRAMMING

Michigan Medicaid does not provide software to billing agents for electronic claims creation. All billing agents must have a way to create or produce electronic files to submit to Michigan Medicaid.
Section 4 - FILE TRANSFER SERVICE (FTS) [former name: DEG]

Michigan’s data-submission portal is the File Transfer Service (FTS); however, it has previously been referred to as the Data Exchange Gateway, or DEG. Some documents may still reference the Data Exchange Gateway (DEG); be aware that a reference to the DEG portal is a reference to the FTS.

MDHHS has established an Internet connection to the FTS, which is a Secure Sockets Layer connection. This connection is independent of the platform used to transmit data.

Billing agents will use the FTS to submit and retrieve files electronically with MDHHS. Every billing agent receives an FTS “mailbox”, which is where their files are stored and maintained. You can access this mailbox to send and retrieve files through the Internet connection.

4.1 FTS - Internet Connection

The https connection to the FTS, using your internet browser, provides secure connection and file transfer over the Internet.

4.1.1 Java and Non-Java Mode

Web-based access to the FTS can be run using Java mode or Non-Java mode. Use of Java mode will provide additional features compared to running in Non-Java mode.

The Chrome internet browser does not support Java, so FTS will run in Non-Java mode when accessed using Chrome. Internet Explorer and Firefox internet browsers will allow the user to run using Java. Consult your organization’s IT support team with questions about the browser available at your work location.

4.1.2 PC Setup

1. You must have an Internet Browser installed on your PC. FTS has been tested on Windows 7 with the following browsers:
   - Internet Explorer 8, 10 and 11
   - Firefox 38
   - Chrome 43

   Note: Using an untested Internet Browser may cause some screens to appear different than the screens you see in this documentation, which are based on Chrome (for Non-Java mode) and Internet Explorer (for Java mode).

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.
4.1.3 Logging onto the MDHHS Internet Connection

1. Log onto https://dxgweb.state.mi.us

2. All Billing Agents must contact MDHHS to obtain unique credentials for accessing the FTS. To logon, enter your MDHHS-assigned billing agent FTS Username in the Username box, such as DCH???? using all caps (where “????” is your unique Username assigned by MDHHS).

3. In the Password box, enter your password. Then, click on the “Logon” button.

4. If you need to have your FTS password reset, please send a password reset request to AutomatedBilling@michigan.gov.
4.1.4 Downloading Files from FTS

Billing agents can download response files from their FTS “mailbox”. These files include TA1, 999 Acknowledgement files, 835 files, etc. Your available messages (files) to download are displayed on the Available tab when you log on.

Check the box next to the “Message ID” you would like to download. Then select one of the following: Download As Zip, Download As Binary or Download As Text, in the dark green band. Once a file downloads, it will no longer appear on the Available tab; you will need to click on the Downloaded tab to re-download previously downloaded files.
4.1.5 Uploading Files to the FTS

1. To start the Uploading process, click on **Upload Message**:

2. The following screen will appear; complete the screen entries (see *Reference Notes*, below) and use the *Choose File* or *Browse...* button to select a file from your PC.

**Non-Java Mode:**
**Java Mode:**

![File Transfer Service](image)

**Reference Notes:**

- **Recipient** will be "DCHEDI" or "DCHBULL" for most files that you are uploading to MDHHS.

- **Class ID** is the MDHHS File Name of the file that you are submitting. Please see *Section 11. CLASS ID/Filename* (formerly, ‘Appl ID Filename’) for a listing of Class ID/File Names (ex.: 5475 is the Class ID/File Name for 837 FFS files). Please note that all test files must use “T” as the fifth digit of the Class ID/File Name (ex.: 5475T).

- **Transfer Mode** needs to be changed to “Text” if Recipient is "DCHEDI".

- **File** is the file that you are submitting to MDHHS through the FTS. You will need to click on the Choose File or Browse... button to select the file to be uploaded from your PC.

1. When you have selected your file, click the Upload button to submit the file.

2. Once the upload has completed, the following display and message will appear:
Non-Java Mode:
**NOTE:** This is **not** your 999 acknowledgement file. If you are submitting a file to MDHHS and would like to verify your return acknowledgement file, you will have to go to the **Available** tab to verify that your 999 acknowledgement file has been returned for each file that you sent. The Class ID/Filename of your 999 is the same Class ID of the file you sent. (Example: An 837 claims file submitted as **5475** would receive a 999 acknowledgement file also named **5475**.)
Section 5 - SSLFTP/SFTP (WS_FTP) SETUP FOR THE FTS

5.1 Overview

This section provides information on how to set up your SSLFTP/SFTP client software to use with the State of Michigan File Transfer Service (FTS). 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 FTS. 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.

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 WS_FTP Professional Version 2007

![Site Options - DEG_New_Prod_sslftp](Image)

![Site Options - DEG_New_Prod_sslftp](Image)
Site Options - DEG_New_Prod_sftp

Advanced

- Server type: FTP/SSL (AUTH SSL)
- Host type: Automatic Detect
- Fjewell: NONE
- Use Passive mode for data connections
- Force passive connections to use host address
- Disable directory caching
- Verify deletions

Connection retries (0 - 40 attempts): 0
Connection retry delay (5 - 300 seconds): 30
Network timeout (5 - 3000 seconds): 65
Remote port (usually 21): 11250
Keep alive (10 - 3600 seconds): 0

OK Cancel Help

Site Options - DEG_New_Prod_sftp

SSL

If your server requires a client certificate for authentication purposes, please select the certificate for this server below.

Client certificate: NONE
- Use at least 128bit SSL for secure connections
- Use unencrypted command channel after SSL authentication
- Use unencrypted data channel
- Use TLSv1 only
- Ignore Command Failures

OK Cancel Help
5.2.4 Example of Site Setup for SFTP (WS_FTP Professional Version 7)
5.2.5 Certificate Screen (Version 2007)

5.2.6 Example of Good Transfer Log

5.2.6.1 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

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

E SM ACA CORE 2017-SEP  Page 23 of 51
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 A
200 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

5.2.6.2 SFTP Transfer Log Example
Connected 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
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 Dirlisting transferred 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
5.3 Connecting Issues

1. If you can’t logon with SSLFTP, make sure you have the right port number 11250 and advanced – 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 (refer to the specification screens and examples above).

5.4 Change File Directories

The following screens provide an example for changing the directory; your software may differ from these images.

Note: Your source file name must be restricted to one of the four- or five-character Class-ID Filenames from the chart in Section 11 of this document (Ex.: “5475” or “5475T”). Test files must always use a “T” as the fifth character of the filename.

1. Use your file transfer manager application (ex.: the Ipswitch WS_FTP tool) to access your destination directory:
2. Enter the desired target Directory name (/DCHEDI) by selecting the indicated (target) directory icon, entering “/DCHEDI” in the pop-up “Change Directory” dialogue box, and clicking the “OK” button:

3. When the new target directory is displayed, transfer your file from the “My Computer” window to the “/DCHEDI” directory, by using one of the following:
   a. Drag the file from the My Computer window and drop it into the /DCHEDI or,
   b. Highlight the file in your My Computer directory, and click the right-pointing arrow.
4. Once the file is moved to /DCHEDI, look in your FTS mailbox for the corresponding response file ("5475", in this example); the Modified date and time will be included in the name of the response file. Response files are typically sent within two hours of your submission; if no response file is received, please contact: AutomatedBilling@michigan.gov.

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 Phase II CORE 270: Connectivity Rule document at the link below for detailed information and specifications for HTTP MIME Multipart and SOAP+WSDL based interactions:


The following diagram depicts the relationship of the transport modes to the submitted transaction.
6.2 System Availability
The MDHHS CHAMPS system is available 24 hours per day, 7 days per week, except for 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, see the Biller “B” Aware page at:

http://michigan.gov/tradingpartners >> Communications and Training >> Medicaid Alerts >> Biller "B" Aware

6.2.1 Real-time Inquiry Response
A response to a real-time inquiry will be provided within 20 seconds during hours of availability.

6.2.2 Batch Inquiry Response
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:
      - Real Time Production: https://corerealtime.state.mi.us/ecams/soap?wsdl
      - Real Time Testing: https://corerealtimeqa.state.mi.us/ecams/soap?wsdl
   b. Submit MIME to:
      - Real Time Production: https://corerealtime.state.mi.us/ecams/multipart
      - Real Time Testing: https://corerealtimeqa.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**

1. **Trading Partner’s CORE Compliant Application**
   - Send Request to

2. **Authentication**
   - INVALID
   - HTTP 403
   - VALID

3. **Valid SenderID, Envelope**
   - INVALID
   - SOAP: HTTP 500
   - MIME: HTTP 200
   - VALID

4. **CHAMPS Processing**

5. **HTTP 200 & 271 or 277**

**SOAP URLs**

- `https://corerealtime.state.mi.us/ecams/soap?wsdl`
- `https://corerealtime.state.mi.us/ecams/multipart`

**Links**

- [https://corerealtime.state.mi.us/ecams/soap?wsdl](https://corerealtime.state.mi.us/ecams/soap?wsdl) (SOAP)
- [https://corerealtime.state.mi.us/ecams/multipart](https://corerealtime.state.mi.us/ecams/multipart) (MIME)
6.3.2 Batch Request and Response Handling

6.3.2.1 Initial Batch Submission

1. The user application submits a batch SOAP or MIME request.
   a. Submit SOAP to:
      Batch Production: https://corebatch.state.mi.us/ecams/soap?wsdl
      Batch Testing: https://corebatchqa.state.mi.us/ecams/soap?wsdl
   b. Submit MIME to:
      Batch Production: https://corebatch.state.mi.us/ecams/multipart
      Batch 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. 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.
6.3.2.2 Batch Process Flow

1. The user application submits a time-delayed batch pickup request.
   a. Submit SOAP to:
      - Batch Production: https://corebatch.state.mi.us/ecams/soap?wsdl
      - Batch Testing: https://corebatchqa.state.mi.us/ecams/soap?wsdl
   b. Submit MIME to:
      - Batch Production: https://corebatch.state.mi.us/ecams/multipart
      - Batch 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. 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
Electronic Submission Manual

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 9:00 pm on a business day, the 271 or 277 response transactions will be available by 7:00 am the next business day.

Note: Multiple interchanges may be returned within the same Payload.

The diagram on the next page depicts the Batch Pickup Process Flow.
6.3.2.4 Batch Pickup Process Flow

Trading Partner's CORE Compliant Application

Send Request to

https://corebatch.state.mi.us/ecams/soap?wsdl (SOAP)
https://corebatch.state.mi.us/ecams/multipart (MIME)

Authentication

VALID

HTTP 202

Valid SenderID, Envelope

VALID

Payload ID exists

Yes

HTTP 200 and 999 or 271 or 277

VALID

HTTP 202

INVALID

HTTP 403

VALID

SOAP: HTTP 500
MIME: HTTP 200

INVALID

999 Batch Acknowledgement or 271 or 277 not available
6.4 Transmission Administrative Procedures

Response Times: A response to a real-time inquiry will be provided within 20 seconds during hours of availability. A response to a batch inquiry submitted by 9:00 pm on a business day will be provided by 7:00 am 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 MDHHS directly to determine if system availability problems exist or if there are known internet traffic constraints causing the delay. Please verify your file contents before any further resubmission.

6.6 Communication Protocols

6.6.1 HTTP MIME Multipart

MDHHS 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

MDHHS 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 + WSDL XML Schema

The XML schema 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Accepted Values</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>PayloadType</td>
<td>X12_270_Request_005010X279A1 X12_005010_Request_Batch_Results_271</td>
<td>Real-time &amp; batch submissions</td>
</tr>
<tr>
<td></td>
<td>X12_276_Request_005010X212 X12_005010_Request_Batch_Results_277</td>
<td>Batch results retrieval for 270/271</td>
</tr>
<tr>
<td></td>
<td>X12_835_Request_005010X221 X12_TA1_Response_00501X231A1</td>
<td>Batch results retrieval for 276/277</td>
</tr>
<tr>
<td></td>
<td>X12_999_Response_005010X231A1</td>
<td>Batch retrieval for 835 (RA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TA1 response (real-time)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>999 response (real-time)</td>
</tr>
<tr>
<td>ProcessingMode</td>
<td>RealTimeBatch</td>
<td>Batch used for either submission or pickup</td>
</tr>
<tr>
<td>PayloadID</td>
<td>PayloadID will conform to ISO UUID standards (described at ftp://ftp.rfceditor.</td>
<td>Generated using a combination of local timestamp (in milliseconds) as</td>
</tr>
<tr>
<td></td>
<td>org/in-notes/rfc4122.txt), with hexadecimal notation.</td>
<td>well as the hardware (MAC) address33, to ensure uniqueness.</td>
</tr>
<tr>
<td>Payload Length</td>
<td>Length of the X12 document</td>
<td>Required only if ProcessingMode is Batch; otherwise do not send.</td>
</tr>
<tr>
<td>TimeStamp</td>
<td>YYYY-MM-DDTHH:MM:SSZ</td>
<td>See: <a href="http://www.w3.org/TR/xmlschema11-2/#dateTime">http://www.w3.org/TR/xmlschema11-2/#dateTime</a></td>
</tr>
<tr>
<td>User Name</td>
<td>MDHHS Assigned</td>
<td>For SOAP+WSDL and MIME Multipart use only.</td>
</tr>
<tr>
<td>Password</td>
<td>MDHHS Assigned</td>
<td>For SOAP+WSDL and MIME Multipart use only.</td>
</tr>
<tr>
<td>SenderID</td>
<td>MDHHS Assigned</td>
<td>This is assigned based on how you are enrolled in CHAMPS. It will be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>your NPI number, Provider ID, or FTS Username ID</td>
</tr>
<tr>
<td>ReceiverID</td>
<td>D00111</td>
<td>This is the Michigan Medicaid receiver ID.</td>
</tr>
<tr>
<td>CORERuleVersion</td>
<td>2.2.0</td>
<td></td>
</tr>
</tbody>
</table>
### Field Accepted Values Comment

<table>
<thead>
<tr>
<th><strong>CheckSum</strong></th>
<th>Checksum of the X12 document</th>
<th>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.</th>
</tr>
</thead>
</table>

| **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.

#### 6.6.4.1 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:


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

#### 6.6.4.2 Envelope Processing Status and Error Codes

When SOAP is used, some of the CORE-compliant Envelope Processing errors map to SOAP Faults; refer to: [https://www.w3.org/TR/soap12-part1/](https://www.w3.org/TR/soap12-part1/)
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 troubleshooting and logging). When an error occurs, PayloadType is set to CoreEnvelopeError.

The following table shows commonly used error codes and descriptions.

<table>
<thead>
<tr>
<th>CORE-compliant Envelope Processing Status/Error Codes (Normative, Comprehensive)</th>
<th>Status Code Description (Intended Use)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>Envelope was processed successfully.</td>
</tr>
<tr>
<td>&lt;FieldName&gt;Illegal</td>
<td>Illegal value provided for &lt;FieldName&gt;.</td>
</tr>
<tr>
<td>&lt;FieldName&gt;Required</td>
<td>The field &lt;FieldName&gt; is required but was not provided.</td>
</tr>
<tr>
<td>&lt;FieldName&gt;NotUnderstood</td>
<td>The field &lt;FieldName&gt; is not understood at the receiver. In the case of SOAP, this error is returned as a NotUnderstood SOAP fault.</td>
</tr>
<tr>
<td>VersionMismatch</td>
<td>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.</td>
</tr>
<tr>
<td>Unauthorized</td>
<td>The username/password or Client certificate could not be verified.</td>
</tr>
<tr>
<td>ChecksumMismatched</td>
<td>The checksum value computed on the recipient did not match the value that was sent in the envelope.</td>
</tr>
<tr>
<td>Sender</td>
<td>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.</td>
</tr>
<tr>
<td>Receiver</td>
<td>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.</td>
</tr>
</tbody>
</table>

Section 7 - PASSWORDS

7.1 SOAP+WSDL and MIME Multipart Passwords

A username and password is required to authenticate the submitted transaction request when using the SOAP+WSDL or MIME Multipart modes. Passwords must be changed every 120 days.

- The Initial request for a SOAP or MIME password must be sent to Automated Billing at: AutomatedBilling@michigan.gov with a subject line of “CORE Password Request”.
- Automated Billing will reply with a temporary password, see 7.1.1 on how to setup a personal password.
- Trading Partners can only reset their password using CHAMPS password maintenance screens. Please note, anyone with a Domain Administrator CHAMPS profile in your organization has the authority to request password resets for your organization.
7.1.1 **Password Maintenance**

To change your personal (or temporary) SOAP or MIME password:

1. Log in to CHAMPS; from the tabs toolbar at the top, select the **My Inbox** tab;
2. Select **EDI Password Maintenance**;
3. Enter your old password, new password, and confirm new password;
4. Choose security questions and answers;
5. Enter the displayed security code in box;
6. Click the **Submit** button in the upper-left portion of the screen.

The **Change Password** screen is shown below:
7.1.2 Password Replacement

To replace a lost SOAP or MIME password, your designated CHAMPS Domain Administrator must request a temporary password as follows:

1. Login to CHAMPS using their Domain Administrator profile;
2. From the tabs toolbar at the top, select the My Inbox tab;
3. Select EDI Forgot Password (shown below);
4. Enter your email address for temporary-password delivery, and click the Go button.

A temporary password will be emailed to the email address you entered on the screen.

The Forgot Password screen is shown below:

---

7.2 SSLFTP/SFTP Passwords

To change the SSLFTP/SFTP password, use the Change Password function within FTS; please refer to section 7.3.
7.3 File Transfer Service (FTS) Passwords

7.3.1 Change Password function

7.3.1.1 Password Restrictions:
Passwords have a minimum length of 8 characters. With at least 1 uppercase character, 1 lowercase character, 1 number and 1 special character.

7.3.2 Unknown Password
An email request to Automated Billing at AutomatedBilling@michigan.gov must come from the Technical Contact listed within CHAMPS.

Section 8 - ELECTRONIC BATCH WEB UPLOAD THROUGH CHAMPS

1. Log on to CHAMPS 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. You will need either the CHAMPS Full Access or Billing Agent Access profile
3. From the tabs toolbar at the top click on My Inbox;
4. Select Upload File from the My Inbox drop-down list;
5. Click the Upload button.
Please click on the Upload button to upload your file.

Please use below naming conventions for web upload files.

**837 Fee For Service:**
1) NPI.5475.CCYYMDDhhmm
2) CHAMPS PROVIDERID.5475.CCYYMDDhhmm

**837 ENC:**
1) NPI.5478.CCYYMDDhhmm
2) CHAMPS PROVIDERID.5478.CCYYMDDhhmm

**270:**
1) NPI.5414.CCYYMDDhhmm
2) CHAMPS PROVIDERID.5414.CCYYMDDhhmm

**276:**
1) NPI.4952.CCYYMDDhhmm
2) CHAMPS PROVIDERID.4952.CCYYMDDhhmm

**278:**
1) NPI.5386.CCYYMDDhhmm
2) CHAMPS PROVIDERID.5386.CCYYMDDhhmm
6. Click the **Choose File** button to select the file on your PC that you wish to submit, then click the **OK** button:

![Choose File Button Example]

**Please note:**

1. The file name must include the Class 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.CCYYMMDDhhmm
     - (example: 1234567890.5475.201210261208.dat)
   - ProviderID.5475.CCYYMMDDhhmm
     - (example: 1234567.5475.201210261209.dat)

3. All web batch files must have an extension of .dat
4. A file size of 50MB 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;
2. Select My Inbox;
3. Select Retrieve Response/Acknowledgement;
4. Use the Retrieve Acknowledgement Response File screen to download your 999.

5. You may choose a filter in the leftmost drop-down box, such as the Upload/Sent Date that you submitted the file. The percent sign (%) may be used as a wildcard when entering a partial search filter value, other than a date.
6. Review your acknowledgement response file to make sure your file was accepted. The acknowledgement will contain the same Class ID/File Name as the file you uploaded.
Section 9 - B2B Testing

Business to Business (B2B) testing is the process of submitting test files to MDHHS for validation, prior to a new business partner receiving approval from MDHHS to submit electronic transactions. This section describes B2B testing for HIPAA v5010 transactions.

MDHHS' testing process consists of two stages for Trading Partners. Only HIPAA 5010 compliant files will be accepted.

9.1 Billing Agent IDs for New Trading Partners

New Trading Partners (who do not already have a billing agent ID with MDHHS) will need to apply for a Billing Agent ID. For more information, please refer to: “HOW TO ENROLL AS A BILLING AGENT” at:

http://michigan.gov/tradingpartners >> Electronic Submissions Transactions >> How to Enroll

9.2 5010 Test Instructions by Transaction

For specifics on testing and the v5010 certification criteria, please review the B2B Testing Instructions (see Section 2 for B2B Testing website location). The summary below will give you an overview of the testing process.

9.3 Stage 1 - Ramp Manager Testing

Integrity testing is required for all new 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 MDHHS’ Trading Partners. More information on integrity testing is available at http://michigan.gov/tradingpartners. You must request enrollment in this test system by sending an email to: AutomatedBilling@michigan.gov.

9.4 Stage 2 - CHAMPS B2B Testing

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 regarding file submission and file naming conventions:

- Section 4 - FILE TRANSFER SERVICE (FTS) [former name: DEG]
- Section 5 - SSLFTP/SFTP (WS_FTP) SETUP FOR THE FTS
- Section 6 - ACA CORE TRANSPORT MODES
- Section 8 - ELECTRONIC BATCH WEB UPLOAD THROUGH CHAMPS
- Section 11 - CLASS ID/Filename

Once a test file is submitted to the FTS, you must send an email, including a contact name, telephone number, and email in your organization, to the B2B Test Team, at: MDHHS-B2B-
Testing@michigan.gov; and to the Automated Billing team at: AutomatedBilling@michigan.gov
to inform MDHHS that a test file has been submitted.

To ensure proper retrieval of your files, use a subject line in your email such as: “5475T Test File DCH????” or “5476T Test File DCH????” where ???? is your MDHHS-assigned FTS Username ID.

Your files will be retrieved and processed through the CHAMPS B2B system. We will not send you a TA1 or 999 Acknowledgment for these files until they have been uploaded to the test environment. Once that is done, you can retrieve your TA1 or 999 in your FTS mailbox.

If you have a question, send an email to the B2B Test Team, at: MDHHS-B2B-Testing@michigan.gov; and the Automated Billing team at: AutomatedBilling@michigan.gov.

Section 10 - 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 MDHHS. MDHHS 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 MDHHS.

Below is an example of an Accepted 999: certain data is removed per HIPAA regulations. The FTS ID has been replaced with ????:

```
ISA*00*00*ZZ*D00111ZZ????*120425*1551*0*P*:~
GS*FA*D00111????*20120425*1551*1*X*005010X231~
ST*999*0001*05010X231~
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~
```
Below is an example of an Accepted 999 with non-fatal errors that was accepted for further processing. Each error is identified in the IK3 and IK4 segments. Please refer to the HIPAA Implementation Guide and the Michigan Companion Guide.

ISA*00* 00* ZZ*D00111 ZZ*???? 120426*1701*^00501*000000001*0*P*:~
GS*FA*D00111*????*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*1~
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 Implementation Guide and Michigan Companion Guide.

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

GS*FA*D00111*????*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:TPRF110600380841~
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~
IK4*2*127*I12*23D01025908~
```
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 11 - CLASS ID/Filename (formerly, ‘Appl ID Filename’)

You will need to use the ‘Class ID Filename’ for files that are submitted through the FTS to MDHHS, and to recognize files that MDHHS returns to your billing agent “mailbox”.

If you wish to submit a file that is not listed, please contact AutomatedBilling@michigan.gov for more information.

<table>
<thead>
<tr>
<th>Class ID Filename*</th>
<th>HIPAA Transaction ID</th>
<th>Transaction Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>5414</td>
<td>270</td>
<td>Medical Eligibility Inquiry</td>
</tr>
<tr>
<td>5415</td>
<td>271</td>
<td>Medical Eligibility Response</td>
</tr>
<tr>
<td>4952</td>
<td>276</td>
<td>Health Care Claim Status Inquiry</td>
</tr>
<tr>
<td>4953</td>
<td>277</td>
<td>Health Care Claim Status Response</td>
</tr>
<tr>
<td>5386</td>
<td>278</td>
<td>Prior Authorization Request (Inbound to MDHHS)</td>
</tr>
<tr>
<td>5383</td>
<td>278</td>
<td>Prior Authorization Response (Outbound from MDHHS)</td>
</tr>
<tr>
<td>4985</td>
<td>820</td>
<td>Payroll Deducted and Other Premium Payment</td>
</tr>
<tr>
<td>4976</td>
<td>834</td>
<td>Card Cutoff Audit File</td>
</tr>
<tr>
<td>5014</td>
<td>834</td>
<td>Card Cutoff File – PIHP and HMP-PIHP</td>
</tr>
<tr>
<td>5015</td>
<td>834</td>
<td>Healthy Kids Dental – EOM/FOM Audit File</td>
</tr>
<tr>
<td>5093</td>
<td>834</td>
<td>HSW Audit File (Habilitation Support Waiver)</td>
</tr>
<tr>
<td>5419</td>
<td>834</td>
<td>MChild-CA EOM/FOM Audit File</td>
</tr>
<tr>
<td>5421</td>
<td>834</td>
<td>MChild-CMH EOM/FOM Audit File</td>
</tr>
<tr>
<td>5485</td>
<td>834</td>
<td>NEMT- Weekly Update - Enrollment</td>
</tr>
<tr>
<td>5610</td>
<td>834</td>
<td>DHIP Update File (DHS Incentive Payment)</td>
</tr>
<tr>
<td>5611</td>
<td>834</td>
<td>AUT Update File</td>
</tr>
<tr>
<td>5629</td>
<td>834</td>
<td>PIHP &amp; HMP-PIHP Update File</td>
</tr>
<tr>
<td>5705</td>
<td>834</td>
<td>Full File Audit File - Integrated Long-Term Care Audit Enrollment File sent to ICOs</td>
</tr>
<tr>
<td>5721</td>
<td>834</td>
<td>Update Transaction File - MI Health Link Daily Enrollment</td>
</tr>
<tr>
<td>5790</td>
<td>834</td>
<td>Daily File – Benefit Enrollment and Maintenance</td>
</tr>
<tr>
<td>4987</td>
<td>835</td>
<td>Health Care Claim Payment and Remittance Advice</td>
</tr>
<tr>
<td>5475</td>
<td>837</td>
<td>FFS Health Care Claims</td>
</tr>
<tr>
<td>5476</td>
<td>837</td>
<td>Encounters Transactions (v5010)</td>
</tr>
<tr>
<td>5477</td>
<td>837</td>
<td>NCPDP Transactions</td>
</tr>
<tr>
<td>5776</td>
<td>837</td>
<td>Medicare ICO Inbound Encounter File (5890 is the ETRR outbound response for the 5776)</td>
</tr>
<tr>
<td>5777</td>
<td>837</td>
<td>Medicaid ICO Inbound Encounter File</td>
</tr>
<tr>
<td>Class ID Filename*</td>
<td>HIPAA Transaction ID</td>
<td>Transaction Information</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>5786</td>
<td></td>
<td>Outbound ICO Medicaid File - response file for 5777</td>
</tr>
<tr>
<td>5848</td>
<td></td>
<td>Medicaid Inbound ICO NCPDP PA4.2 - Medicaid file</td>
</tr>
<tr>
<td>5849</td>
<td></td>
<td>Outbound Medicaid ICO NCPDP - response file for 5848</td>
</tr>
<tr>
<td>5850</td>
<td></td>
<td>Medicare ICO NCPDP Inbound Encounter file</td>
</tr>
<tr>
<td>5852</td>
<td></td>
<td>MHP Inbound NCPDP file</td>
</tr>
<tr>
<td>5853</td>
<td></td>
<td>Outbound MHP NCPDP - response file for 5852</td>
</tr>
<tr>
<td>5877</td>
<td></td>
<td>PIHP Daily Enrollment File</td>
</tr>
<tr>
<td>5890</td>
<td></td>
<td>ETRR outbound response for the 5776 Medicare ICO Inbound Encounter File</td>
</tr>
</tbody>
</table>

11.1 *Notes Regarding TEST Files

1. You must place a “T” in the fifth position of the Class ID Filename to identify a test file, for example 5414T.
2. A “T” must also be placed in the ISA15 data element within the header record of a 270, 276, 278, or 837 test file.
3. The transactions in a test file will not post to the production CHAMPS system; test files will only be routed to the CHAMPS B2B system.
4. A valid Sender ID must appear in the ISA06 and GS02 data elements, for the test system to be able to identify you as the file submitter and to return the response file to your FTS mailbox. If you do not receive a response file within two hours, verify the syntax of the test file in Ramp Manager. If it passes Ramp Manager and you still don’t receive a response file contact the B2B Test team at: MDHHS-B2B-Testing@michigan.gov.