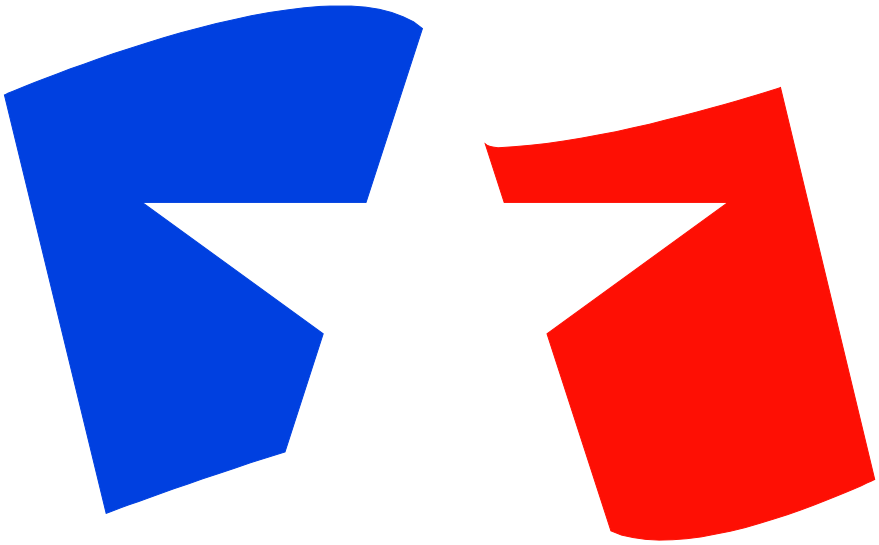


TMHP

TEXAS MEDICAID
&
HEALTHCARE PARTNERSHIP

A STATE MEDICAID CONTRACTOR

EDI CONNECTIVITY GUIDE

TABLE OF CONTENTS

1 Introduction 3
2 TMHP Electronic Transactions 4
2.1 EDI Transactions 4
2.2 TMHP Receiver ID Numbers 5
3 Technology Requirements 7
3.1 Telecommunications 7
3.2 File Compression Techniques 7
3.3 File Transfer Protocol (FTP) Requirements 7
4 Establishing a Connection to TMHP 8
4.1 Installation Requirements 8
4.2 Connecting to TMHP Using the Cisco AnyConnect VPN Instructions 8
5 File Transfer Protocol 9
5.1 FTP Instructions – Microsoft Windows Explorer 9
6 Safe Harbor Connection 12
6.1 Connectivity Standards 12
6.1.1 Hypertext Transfer Protocol/Secure (HTTPS) Multipurpose Internet Mail Extensions (MIME) Multipart 12
6.1.2 Simple Object Access Protocol (SOAP) + Web Service Definition Language (WSDL) 13
6.1.3 SSL Certificates/TLS Version 14
6.1.4 835 File Retrieval via Safe Harbor Connectivity 14
7 Hyper-Text Transfer Protocol (HTTP) Instructions 15
8 TMHP File Naming conventions 16
8.1 Files Sent To TMHP 16
8.2 Files Sent From TMHP 16
9 Contacting TMHP Electronic Data Interchange Support 18
9.1 Enrollment and Testing Information 18
10 Appendices 19
10.1 Appendix A – Microsoft DOS-based FTP Client Program 19
10.2 Appendix B – WS_FTP PRO 20
10.3 Appendix C – Safe Harbor Connection 22
10.3.1 Connectivity Standards 22
10.3.2 Error Reporting 23
10.4 Appendix D: TMHP Certificate Signature Request Instructions 26
11 Change Log 28

1 Introduction

The Texas Medicaid & Healthcare Partnership (TMHP) is made up of a team of contractors that process Texas Medicaid electronic data interchange (EDI) transactions under contract with the Texas Health and Human Services Commission (HHSC.)

Acute Care, Long Term Care (LTC) and Long Term Services and Support (LTSS) transactions are accepted electronically into TMHP EDI via file transfer protocol (FTP). Acute care transactions are processed through Compass21, and Long Term Care transactions are processed through the Claims Management System (CMS) Long Term Care. LTSS claims are forwarded to the Managed Care Organizations (MCOs) for processing.

Additionally, TIERS eligibility information is available as an interface through TMHP EDI FTP and Safe Harbor connection methods.

The purpose of this guide is to outline the procedures for submitting transactions and retrieving responses and reports.

Note: This guide does not apply to TexMedConnect users or Care Forms users.

Audience

This guide is intended for trading partner use in conjunction with the following guides:

- American National Standards Institute (ANSI) X12N 5010 Implementation Guides which are available on the Washington Publishing Company web site at http://www.wpc-edi.com
- The TMHP Companion Guides which are available on the TMHP-EDI Testing web page at https://editesting.tmhp.com/index.jsp and on the TMHP EDI web page at http://www.tmhp.com/Pages/EDI/EDI_companion_guides.aspx under “Reference Materials.”

A “trading partner” is defined as any entity trading data with TMHP EDI. Trading partners include vendors, clearinghouses, providers (other than those using TexMedConnect), and billing agents.

2 TMHP Electronic Transactions

2.1 EDI Transactions

The following electronic transactions are available through TMHP:

Inbound Transaction	Inbound Format	Response	Response Format	Comments
270 Eligibility Inquiry	ANSI X12 5010	271 Eligibility Response	ANSI X12 5010	Acute Care
				Long Term Care
276 Claim Status Inquiry	ANSI X12 5010	277 Claim Status Response	ANSI X12 5010	Acute Care/Long Term Care
	Proprietary	CSI Supplemental	Proprietary	Long Term Care
278 Request for Review	ANSI X12 5010	278 Response	ANSI X12 5010	Acute Care
				Long Term Care
275 Additional Information to Support a Health Care Service Review	ANSI X12 5010	824 Response	ANSI X12 5010	Long Term Care
837 Professional Claim	ANSI X12 5010	277CA Claims Acknowledgement /277CAU Claims Acknowledgement from MCO forwarded claims	ANSI X12 5010	Acute Care
				Long Term Care
837 Institutional Claim	ANSI X12 5010	277CA Claims Acknowledgement /277CAU Claims Acknowledgement from MCO forwarded claims	ANSI X12 5010	Acute Care
				Long Term Care
837 Dental Claim	ANSI X12 5010	277CA Claims Acknowledgement /277CAU Claims Acknowledgement	ANSI X12 5010	Acute Care
				Long Term Care

Inbound Transaction	Inbound Format	Response	Response Format	Comments
		from MCO forwarded claims		

Inbound Transaction	Inbound Format	Response	Response Format	Comments
N/A	N/A	835 Electronic Remittance & Status	ANSI X12 5010	Acute Care
N/A	N/A			Long Term Care
N/A	N/A	277P Claim Activity	ANSI X12 5010	Acute Care
N/A	N/A			Long Term Care
N/A	N/A	Financial Supplemental	Proprietary	Long Term Care

2.2 TMHP Receiver ID Numbers

Trading partners should use the following TMHP Receiver IDs/qualifier:

Acute Care

Type	ID Number/Qualifier
TMHP Production Receiver ID:	617591011C21P
TMHP Test Receiver ID:	617591011C21T
ISA07, Interchange Receiver ID Qualifier	ZZ

Long Term Care

Type	ID Number/Qualifier
TMHP Production Receiver ID:	617591011CMSP
TMHP Production Receiver ID/ PASRR- NFSS Form	617591011LTCPP
TMHP Test Receiver ID:	617591011CMST

TMHP Test Receiver ID/ PASRR- NFSS Form	617591011LTCPT
ISA07, Interchange Receiver ID Qualifier	ZZ

TMHP TIERS Eligibility Interface

Type	ID Number/Qualifier
TMHP Production Receiver ID:	617591011TIELP
TMHP Test Receiver ID:	617591011TIELT
ISA07, Interchange Receiver ID Qualifier	ZZ

LTSS (Long Term Services and Support)

Type	ID Number/Qualifier
TMHP Production Receiver ID:	617591011LTSSP
TMHP Test Receiver ID:	617591011LTSST
ISA07, Interchange Receiver ID Qualifier	ZZ

3 Technology Requirements

3.1 Telecommunications

TMHP supports the TMHP virtual private network (VPN) Client, using a high-speed internet connection, to connect to the TMHP network.

For trading partners with a high-speed internet connection, TMHP recommends connecting to the TMHP network over the public internet using the Cisco AnyConnect Secure Mobility Client provided by TMHP.

3.2 File Compression Techniques

TMHP accepts compressed files with PKZIP or WINZIP compression techniques for zip files as well as non-compressed files.

3.3 File Transfer Protocol (FTP) Requirements

TMHP requires FTP as the method for transferring files and retrieving responses. As a result, providers do not need other communication software packages (e.g. XMODEM, YMODEM, ZMODEM, or Kermit) to transfer files.

4 Establishing a Connection to TMHP

4.1 Installation Requirements

These instructions were written for persons running Windows 7 with Internet Explorer. The use of any other operating systems or web-browsers will follow similar steps; however, support using any other operating system or web-browser will be best effort only.

Providers will need to have elevated privileges or permissions to install software onto the machine used for AnyConnect.

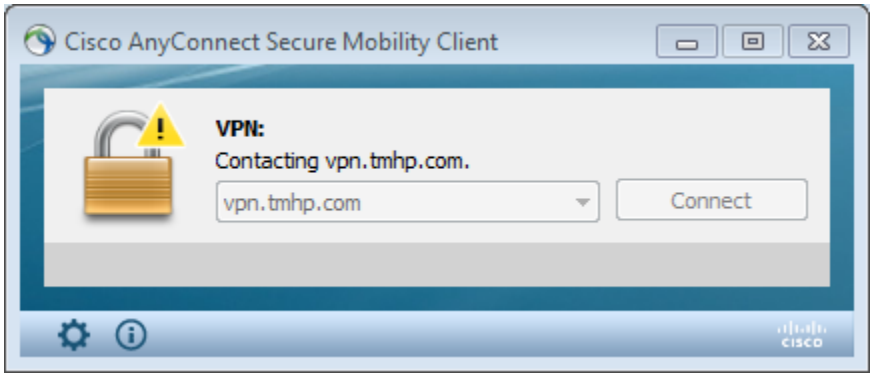
In order to connect into TMHP using the new VPN solution called AnyConnect, providers must follow these instructions:

1. Disconnect VPN session
2. Open Internet Explorer
3. Click on http://vpndownload.tmhp.com/client/anyconnect.zip.
4. Open anyconnect.zip and follow the provided installation instructions from launch screen section.
5. After the installation process is complete, the user will be connected to TMHP using the Cisco AnyConnect VPN.

4.2 Connecting to TMHP Using the Cisco AnyConnect VPN Instructions

After installing the Cisco AnyConnect VPN Client, the user will be able to connect to TMHP for EDI transactions. Follow these instructions to connect with the Cisco AnyConnect VPN client:

1. Go to All Programs>Cisco>Cisco AnyConnect Secure Mobility Client>Cisco AnyConnect Secure Mobility Client. The Cisco AnyConnect VPN client window will appear.



2. Select **TMHP_EDI_VPN** from the Group drop-down menu. Enter the user name in the user name field, without tmhp.net in front of it. Enter the tmhp.net network password in the Password field.
3. Click **Connect**. The Cisco AnyConnect VPN identification window will be displayed.

5 File Transfer Protocol

Once the user is connected to the TMHP Network using a VPN connection, the user is ready to transfer or retrieve files using FTP.

The FTP servers run 24 hours a day, 7 days a week. This availability is subject to scheduled and unscheduled host downtime. According to operational policy, preventive maintenance periods will be scheduled on weekends whenever possible.

To logon to the TMHP FTP server, the user will need an FTP client program or Microsoft Windows Explorer. Microsoft Windows Explorer Version 5.0 and later has built-in FTP functionality. In addition, there are many FTP client programs available either commercially or as internet downloadable shareware (e.g. WS_FTP Pro, etcetera,)

5.1 FTP Instructions – Microsoft Windows Explorer

The instructions below are based on accessing the TMHP EDI FTP server using Microsoft Windows Explorer.

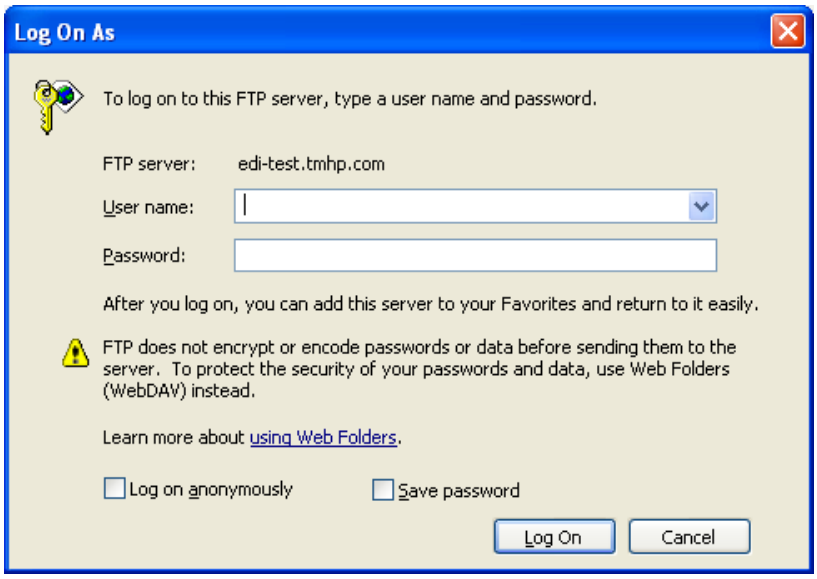
Refer to: Section 9.0, “Appendices,” at the end of this document for instructions about other FTP methods.

Logging on to the TMHP EDI FTP Server

1. Open Microsoft Windows Explorer (5.0 or above). In the address line, type one of the following as applicable:

Environment	Location
Production	ftp://edi.tmhp.com
5010 test	ftp://edi-5010test.tmhp.com

2. In the menu bar, click **File/Login As**, then enter the user's Submitter ID and Password at the User Name and Password prompt. Click **Logon**.



Note: Users who experience problems with their Submitter IDs or passwords can contact the TMHP-EDI Helpdesk by telephone at 1-888-863-3638 or by using the TMHP Contact web page to submit an email.

Uploading Files

1. Once the user is logged on (as described above in Connecting to TMHP) a window will display with the following two folders: Download and Dropbox. These folders are located in the user's home directory.
2. Move the file to be transferred to TMHP by dragging and dropping, or copying and pasting the file to the user's home directory.

Note: The directory path will not display "/home"; instead, the directory path will display both "/dropbox" and "/download folders."

3. The last step is to rename the file that was uploaded, and move it from the user's home directory into the "/dropbox" directory. When the file has finished uploading to the user's home directory, right click on the filename and click Rename. The filename will be highlighted. Rename the file to any name that is different from the original filename. For example, original filename: "12345678.txt", new filename: "12345678.dat". Rename the file with the "/dropbox" path as part of the filename. (For example: /dropbox/12345678.dat). This command moves the file into the dropbox for processing. Another way to move the file is to drag and drop the renamed file, 12345678.dat, into the "/dropbox" folder.

Downloading Files

1. Once the user is logged on (as described above in "Connecting to TMHP") a window will display with the following two folders: "download" and "dropbox." The download folder will be used for retrieving files from TMHP.

2. Double click on the download folder to determine if there are any files to download. To download, right-click on the file and then click **Copy to Folder**. In the pop-up window that appears, choose the appropriate location for the file on your local drive.

6 Safe Harbor Connection

Texas Medicaid & Healthcare Partnership (TMHP) has implemented federally mandated CAQH CORE operating rules for (batch and real-time) eligibility, benefits, claims, claim status and response, and electronic remittance transactions.

Note: Real-time is available for Eligibility Verification (270/271), Claims Status and Response (CSI – 276/277) and Prior Authorization Request for Review (278) transaction types.

A signed agreement is required prior to submitting real-time transactions. Please contact the EDI Helpdesk to initiate a request to submit real-time transactions.

6.1 Connectivity Standards

TMHP supports both transport methods for Safe Harbor Connectivity under the CAQH CORE Operating Rule connectivity versions, 2.2.0 and 4.0.0.

Version 4.0.0 requires the use of a TMHP issued SSL X.509 Certificate. To request a certificate from TMHP, refer to Appendix D: TMHP Certificate Signature Request Instructions.

See Appendix C – Safe Connection for Error Reporting and Messages.

6.1.1 Hypertext Transfer Protocol/Secure (HTTPS) Multipurpose Internet Mail Extensions (MIME) Multipart

Type	ID Number/Location
Acute Care TMHP Receiver ID	617591011C21T
Long Term Care TMHP Receiver ID	617591011CMST
TMHP TIERS Eligibility Interface TMHP Receiver ID	617591011TIELT
Test files CORE Envelope version 2.2.0	https://services-uat.tmhp.com/corerules/httpsrequest
Test files CORE Envelope version 4.0.0	https://coreservices-uat.tmhp.com/corerules/v4/httpsrequest

Type	ID Number/Location
Acute Care TMHP Receiver ID	617591011C21P
Long Term Care TMHP Receiver ID	617591011CMSP

TMHP TIERS Eligibility Interface TMHP Receiver ID	617591011TIELP
Production files CORE Envelope version 2.2.0	https://services.tmhp.com/corerules/httpsrequest
Production files CORE Envelope version 4.0.0	https://coreservices.tmhp.com/corerules/v4/httpsrequest

6.1.2 Simple Object Access Protocol (SOAP) + Web Service Definition Language (WSDL)

Type	ID Number/Location
Acute Care TMHP Receiver ID	617591011C21T
Long Term Care TMHP Receiver ID	617591011CMST
TMHP TIERS Eligibility Interface TMHP Receiver ID	617591011TIELT
Test files CORE Envelope version 2.2.0	https://services-uat.tmhp.com/corerules/soaprequest
Test files CORE Envelope version 4.0.0	https://coreservices-uat.tmhp.com/corerules/v4/soaprequest

Type	ID Number/Location
Acute Care TMHP Receiver ID	617591011C21P
Long Term Care TMHP Receiver ID	617591011CMSP
TMHP TIERS Eligibility Interface TMHP Receiver ID	617591011TIELP
Production files CORE Envelope version 2.2.0	https://services.tmhp.com/corerules/soaprequest
Production files CORE Envelope version 4.0.0	https://coreservices.tmhp.com/corerules/v4/soaprequest

When using SOAPUI, if you are having difficulty connecting, note these two options:

1. If you are creating a new project in SOAPUI, if it returns with an IP address, you must add '?WSDL' to the endpoint of the URL Test and/or Production addresses. (e.g. https://services.tmhp.com/corerules/soaprequest?WSDL)
2. Connectivity version 2.2.0—Install the following files:

   WSDL and XSD for version 2.2

3. Connectivity version 4.0.0—Install the following files:

   WSDL and XSD for version 4.0.0

6.1.3 SSL Certificates/TLS Version

In order to achieve a successful secure handshake process using SSL certificates, clients need to use TLS version 1.2 and obtain and install two public key certificates (Public Primary Root Certification Authority and Intermediate Certification Authority) on their system:

Certificates can be obtained at the following URLs:

- Public Primary Root Certification Authority

  https://www.websecurity.symantec.com/content/dam/websitesecurity/support/digicert/symantec/root/DigiCert_Global_G2.pem

- Intermediate Certification Authority

  https://www.websecurity.symantec.com/content/dam/websitesecurity/support/digicert/symantec/ica/DigiCertGlobalCAG2.pem

Upon obtaining the SSL certificates, connectivity is supported using either the HTTP/S MIME Multipart version 1.1 or SOAP + WSDL version 1.2 methods.

6.1.4 835 File Retrieval via Safe Harbor Connectivity

The request structure only allows one file to be picked up at a time. When retrieving an 835 file via Safe Harbor Connectivity, follow these steps:

1. Use the PayloadType X12_835_Request_005010X221A1 in a batch request to retrieve an 835 file. A successful retrieval will contain the PayloadType 'X12_835_Response_005010X221A1' in the response – with the 835 attached as the Payload.

Requests	Responses
X12_835_Request_005010X221A1	X12_835_Response_005010X221A1 or
	X12_005010_Response_NoBatchResultsFile or
	CORE Envelope Processing Errors See details in Section 10.3.2.
X12_999_SubmissionRequest_005010X231A1	X12_Response_ConfirmReceiptReceived or
	CORE Envelope Processing Errors See details in Section 10.3.2.

2. Send subsequent 835 retrieval requests to retrieve more 835 files. When there are no more 835 files in the submitter folder, the response will contain a PayloadType of 'X12_005010_Response_NoBatchResultsFile' with an ErrorMessage of 'There is no result file ready for pickup.' NOTE: It is important to keep requesting 835 files until you receive this message. Until the message is received, there are more files available for you to retrieve.

Note: 835 retrieval uses Batch processing mode only, and not real time.

7 Hyper-Text Transfer Protocol (HTTP) Instructions

HTTP is the protocol to use to submit interactive files. The submitter will post their valid X12 transactions to the following sites:

File Type	Location
Production files	http://edi-web.tmhp.com/TMHP/Request
Test files	http://edi-webtest.tmhp.com/TMHP/Request

Posting Real-Time Transactions

A signed agreement is required prior to submitting real-time transactions. Please contact the EDI Helpdesk to initiate a request to submit real-time transactions.

To post production files:

1. Open Microsoft Internet Explorer and enter the following TMHP EDI Web Server URL in your Web browser: http://edi-web.tmhp.com/TMHP/Request. The browser builds an HTTP request and sends it to the Internet Protocol address (IP address) indicated by the URL.
2. Post the transaction on Port 80 as a text message in the ANSI 5010 X12 format. Do not include headers, trailers, HTML tags, etc.

The post to the URL is synchronous (e.g. the response to the request is returned to the same session the request was submitted on). If there are errors, a negative 999 or TA1 response file will be returned to the submitter. Errors that are not related to HIPAA or message formatting will cause a timeout for the submitter. Submitters should set the timeout interval at 30 seconds.

8 TMHP File Naming conventions

8.1 Files Sent To TMHP

Trading partners must send files with a ".dat" or ".zip" file extension. Once TMHP receives the file, TMHP will rename the file with a unique TMHP-assigned Batch ID.

Note: Do not send path information with the ".zip" files. If the path information is submitted, the files will error and no response files will be returned to the submitter.

8.2 Files Sent From TMHP

TMHP uses a specific naming convention for downloadable files. The format for files the user will retrieve from TMHP is as follows:

- The first 9 digits of the name on downloadable outbound files is the Submitter ID.
- The second 8 characters are the TMHP assigned alpha numeric Batch ID.
- The last 3 characters represent the file extension.

Example: The filename, "123456789.D1234567.999" consists of the 9-digit Submitter ID "123456789," Batch ID "D1234567," and the file extension ".999."

The following table lists the TMHP file extensions and their descriptions:

Transaction	File Extension	Description
Batch ID Report	BID	Report that identifies the TMHP assigned Batch ID. The .BID filename includes the TMHP assigned Batch ID which may be utilized for tracking purposes. The naming convention for this file is: Submitter ID + Batch ID + Filename + .BID. (For Example: 987654321.D44083FS.12345678.dat.BID. In this example, the TMHP Batch ID is D44083FS). For zip files, the filename within the zip file will be sent back to the submitter inside the .BID file.
Functional Acknowledgement	999	File acknowledgement for CMS, C21 and TIERS eligibility interface through TMHP.
Application Reporting	824	For non-claims. Reports errors that are outside of 999 error-reporting, and to report results of an application system's data content edits of transaction sets.
Eligibility Inquiry Response	271	Response to the 270 for CMS, C21 and TIERS
Prior Authorizations	278	Response to the 278 Request for Review

Transaction	File Extension	Description
Claim Status Inquiry	277	Response to the solicited 276 for CMS and C21.
Claims Acknowledgement	277CA	Response to the 837 for C21, CMS, and Encounter claims.
	277CAU	Response for claims forwarded to MCOs
Claim Payment Advice	835	Weekly finalized claim remittance for CMS and C21.
Pending R&S (Claim Activity)	277	Weekly pending claim remittance for CMS and C21.
CMS CSI Supplemental File	Z03	CMS (LTC) Supplemental File that contains claim status data not covered by HIPAA.
CMS Financial Supplemental File	Z04	CMS (LTC) Supplemental File that contains financial data not covered by HIPAA.

9 Contacting TMHP Electronic Data Interchange Support

The TMHP EDI Help Desk assists users with questions about electronic submissions. Providers can contact the TMHP-EDI Helpdesk by telephone at 1-888-863-3638 or by using the TMHP Contact web page to submit an email

9.1 Enrollment and Testing Information

Testing must be completed successfully in order to submit transactions to TMHP. A trading partner agreement must be completed prior to testing.

Note: TexMedConnect users are not required to complete testing before submitting transactions to TMHP.

To facilitate provider testing, TMHP has made Edifecs, a web-based self-testing tool, available to all providers and trading partners. Once a trading partner has received a "Testing Invite Letter" with the assigned user ID and password, the user can log on to http://editesting.tmhp.com. Trading partners can download and sign a Trading Partner Agreement, download companion guide(s), and then test and validate their HIPAA-compliant transactions. Users must download and submit a signed Trading Partner Agreement before testing.

If a trading partner has not received a user ID and password, the user can register at http://editesting.tmhp.com. TMHP will generate an email letter to the trading partner with the user ID and password to use when logging on to the Edifecs site.

The following submitters, vendors, and clearinghouses must complete testing:

1. Submitters that plan to submit transactions directly (e.g. through their own system and not through a vendor or clearinghouse) to TMHP, are required to sign a Trading Partner Agreement and successfully test on the TMHP Edifecs site.
2. Software vendors that plan to submit transactions to TMHP are required to sign a Trading Partner Agreement and successfully test on the TMHP Edifecs site.
3. Software vendors that do not plan to submit transactions to TMHP but have clients who submit transactions to TMHP do not need to sign a Trading Partner Agreement, but they must test on the TMHP Edifecs site. Clients of these Software Vendors must sign a Trading Partner Agreement and successfully test with TMHP.
4. Clearinghouses that plan to submit transactions to TMHP are required to sign a Trading Partner Agreement and successfully test on the TMHP Edifecs site.

Note: Real-Time submitters who have been approved for Real-Time transactions will need to follow the batch testing process through Edifecs with subsequent testing for Real-Time submissions.

10 Appendices

10.1 Appendix A – Microsoft DOS-based FTP Client Program

FTP Instructions

1. Open a DOS prompt (start/run/cmd or start/run/command).
2. Type one of the following as appropriate, press ENTER, and the DOS window will display connection information.:

Environment	Location
Production	>ftp edi.tmhp.com
5010 test	>ftp edi-5010test.tmhp.com

3. Type the Submitter ID at the User prompt, and press ENTER.
4. Type the Password, and press ENTER.

Note: Users can only send and retrieve files using the Submitter ID with which they are logged in. Users who have multiple Submitter IDs must begin a new FTP session for each Submitter ID.

Uploading files using FTP after connecting to TMHP

1. After typing in the Submitter ID and Password, an “ftp>” prompt will be displayed, and the user is logged in to his/her home directory.
2. Files must be transmitted in binary mode. To transfer files in binary mode, type **bin** and press ENTER. A message will display “200 Type set to I.”
3. To verify that there are no more files remaining to be moved to dropbox, type **dir** and press ENTER to display the contents of the home directory.
4. Type **put [yourfilename.dat] [yourfilename.dat]** and press ENTER.

   Note: The “put” command moves the file from the user’s home directory to the FTP directory; <yourfilename> is the name of the file to be transmitted. The second entry of <yourfilename> can be the same as the first <yourfilename> or enter a different name (e.g., **put <A12345.txt> <A12345.dat>**). Files must be sent with a “.dat” or a “.zip” extension. Do not send path information with the “.zip” files. If the path information is submitted, the files will error and no response files will be returned to the submitter.

5. Then use the following rename command to move the file to the upload directory:
   ftp> rename [filename.dat] \dropbox\filename.dat

   Note: Files must be uploaded to the default directory and then renamed to the dropbox directory. Uploading directly to the dropbox may cause incomplete files to be submitted.

Downloading files using FTP after connecting to TMHP

1. After typing in the Submitter ID and Password, an "ftp>" prompt will be displayed, and the user is logged into his/her home directory.
2. Files must be transmitted in binary mode. To transfer files in binary mode, type **bin**, and press ENTER.
3. To verify that there are no more files remaining to be moved to dropbox, type **dir,** and press ENTER to display the contents of the home directory.
4. Type **cd** to change directory to "\download\Batch."
5. Identify the file to be downloaded, type **get** and the filename, and then press ENTER (e.g., ftp> get 12345678.999). When the download is complete, a "Transmission Successful" message will appear.

Note: The file name must exactly match the file name in the home directory.

Logging Off

1. Exit the FTP process by typing **quit** at the "ftp>" prompt and pressing ENTER.
2. Exit the DOS window by typing **exit** at the prompt and pressing ENTER.
3. End the TMHP connection by clicking the modem icon at the bottom right of the screen. The Connection Status window will appear. Click the button to disconnect.

10.2 Appendix B – WS_FTP PRO

When WS_FTP Pro starts, the Connect to Remote Site window will appear on top of the application. Use this window to create a site profile and make the FTP connection.

Note: If this dialog does not appear when the application starts, select Connect from the File menu on the Classic interface of WS_FTP Pro.

To create a site profile in WS_FTP Pro using the New Site Wizard, follow these instructions:

1. Select the MySites folder from the Sites list.

2. Click the **Create Site** button.

The New Site Wizard will appear. To set up a site profile:

1. In the Name box, type a name to use for the connection.
2. **MySites** should appear in the Create In box.
   Note: *If anything other than **MySites** is in the Create In box, click the **Browse...** box and select **MySites** from the list.*
3. Click the **Next >** button.
4. In the **Host Name** or **IP Address** box, type:

Batch	URL	IP
Production	ftp://edi.tmhp.com	67.67.201.175
Regression	ftp://edi-5010test.tmhp.com	67.67.201.73

5. Click the **Next >** button.
6. In the User ID box, enter the current Submitter ID.>
7. In the Password box, enter the assigned Password.
8. Select the **Save Password** option.
9. Click **Finish**.

The newly created TMHP site profile will appear in the **MySites** folder.

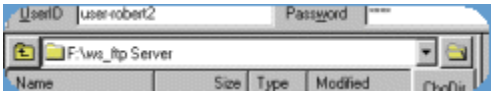
To make the FTP connection:

1. Select the TMHP site name assigned in the **MySites** folder.
2. Click the Connect button.

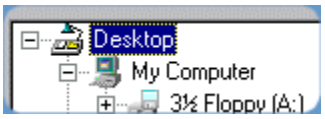
The **Connect to Remote Host** window closes and **WS_FTP Pro** will attempt to make the FTP connection.

To download a file:

1. Choose the folder to which the file will be downloaded (the transfer destination). Use the **Local System** pane of the **WS_FTP Pro** window on the left side of the screen.



2. Click the folder button to the right of the current directory box. The **Browse for Folder** dialog appears.
3. Click on the folder where the file is located.



4. Click the **OK** button at the bottom of the **Browse for Folder** dialog.

The contents of the folder will now be in the **Local System** box. This is the place the downloaded file will be stored.

Look at the list in the right pane of the **WS_FTP Pro** window. This is the **Remote System** list. You will see a display with the following two folders: **download** and **dropbox**.

To upload a file

1. Click on the **dropbox** folder.
2. Select the file to be uploaded.
3. Click the **upload** arrow between the two panes. (This is the green arrow that points to the right.) The **Transfer Manager** will appear showing the status of the transfer.
4. When the transfer is complete, the text on the **Transfer Manager** will show that the transfer has 'finished.' When the transfer is finished, click back on the **WS_FTP Pro** window.

To download a file:

To download files, choose the download folder in the right-hand window of **WS_FTP Pro**. The download folder will be used for retrieving files from TMHP.

1. Double click on the download folder to determine if there are any files to download.
2. Select the file you wish to download.

4. The Transfer Manager appears showing the status of the transfer.

When the transfer is complete, the text on the **Transfer Manager** will show that the transfer has 'finished.'

10.3 Appendix C – Safe Harbor Connection

10.3.1 Connectivity Standards

Texas Medicaid Healthcare & Partnership (TMHP) provides Safe Harbor transport methods over the public internet for the following transactions:

Core version 2.2

- 270/271 Health Care Eligibility Benefit Inquiry and Response
- 276/277 Health Care Claim Status Request and Response
- 835 Retrieval of Health Care Claim Payment/Advice

Additional transactions added for CORE 4.0.0

- 837/277CA Health Care Claim: Institutional
- 837/277CA Health Care Claim: Professional
- 837/277CA Health Care Claim: Dental

Note: 277CAU MCO Claims Acknowledgement retrieval needs to be completed using the FTP connection described in section 5 of this document.

TMHP supports the conformance requirements for the Committee for Affordable Quality Health Care (CAQH), Committee on Operating Rules for Information Exchange (CORE®) Connectivity Standards under CORE Rules 2.2.0 and 4.0.0:

Message Envelope Standards

- HTTP/S MIME Multipart version 1.1
- SOAP + WSDL version 1.2

Submitter Authentication Standards

- Exchange of Security Identifiers
- User ID and Password authentication must be encrypted by the HTTP/S protocol
- Communications-level Errors and Acknowledgements

Safe Harbor Connectivity

- Conformance to information transportation and message standards, along with response and availability ensure safe harbor for electronic transactions

Safe Harbor addresses transport level to message envelope level, message envelope metadata, message envelope standards and submitter authentication standards for both batch and real-time transactions, along with communications-levels errors and acknowledgements.

10.3.2 Error Reporting

Errors associated with connectivity, authentication, authorization, etc., are reported at this level.

Error Code/Message	Connectivity/Authentication Level Errors
HTTP 200 OK	Request Successfully Received and Accepted
HTTP 202 Accepted	Batch Submission Accepted
HTTP 403 Authentication Error	Authentication Failed. Please Verify Username and Password.
HTTP 500 Internal Server Error	Unexpected Error During Processing. Please Try Again Later.

For successful Batch submissions, ‘Success’ is returned in the ErrorCode field and the Batch ID is returned in the ErrorMessage field. TMHP recommends that submitters keep a record of this information for support requests.

Errors associated with structure or data included within the body of the message are reported at this level.

Note: All CORE envelope field names are case-sensitive. (i.e. CheckSum, PayloadID, PayloadLength, Payload, PayloadType, ProcessingMode, ReceiverID, and SenderID.)

Error Code	Error Message	Resolution
CheckSumMismatch	Illegal value provided for CheckSum. (For batch only.)	Check that the CheckSum is correct for the Payload request. (Algorithm is SHA-1 and Encoding is Hex.)
CheckSumRequired	The field CheckSum is required, but was not provided. (For batch only.)	Check that the field name is spelled correctly and that a value exists.
PayloadIDIllegal	Duplicate PayloadID sent by submitter.	Check that the PayloadID is unique.
PayloadIDIllegal	PayloadID not found. (For batch only.)	Check that the PayloadID used in a batch retrieval request is associated to a batch submission.
PayloadIDRequired	The field PayloadID is required, but was not provided.	Check that the field name is spelled correctly and that a value exists.
PayloadLengthIllegal	Illegal file size provided for PayloadLength. (For batch only.)	Check that the value is less than the reject threshold.
PayloadLengthRequired	The field PayloadLength is required, but was not provided. (For batch only)	Check that the field name is spelled correctly and that a value exists.
PayloadRequired	The field Payload is required, but was not provided.	Check that the field name is spelled correctly and that a value exists.
PayloadTypeIllegal	Illegal value provided for PayloadType.	Check that a valid value is specified for

		PayloadType. TMHP supports the following: X12_270_Request_005010X279A1 X12_276_Request_005010X212 X12_835_Request_005010X221A1 X12_999_SubmissionRequest_005010X231A1 X12_TA1_SubmissionRequest_005010X231A1 X12_999_RetrievalRequest_005010X231A1 X12_005010_Request_Batch_Results_271 X12_005010_Request_Batch_Results_277 The below are only available under CORE Rule 4.0.0: X12_837_Request_005010X223A1_2 X12_837_Request_005010X222A1 X12_837_Request_ 005010X224A2
PayloadTypeRequired	The field PayloadType is required, but was not provided.	Check that the field name is spelled correctly and that a value exists.
ProcessingModeIllegal	Illegal value provided for ProcessingMode.	Only 'RealTime' or 'Batch' values are accepted.
ProcessingModeRequired	The field ProcessingMode is required, but was not provided.	Check that the field name is spelled correctly and that a value exists.
ReceiverIDIllegal	Illegal value provided for ReceiverID.	Check that the ReceiverID value in the request is identical to the ReceiverID in the Payload.
ReceiverIDRequired	The field ReceiverID is required, but was not provided.	Check that the field name is spelled correctly and that a value exists.
Sender	The PayloadType and the contents of the Payload did not conform to the expected format.	Check that the PayloadType specified in the request and the GS08 segment in the Payload are compatible. E.g. **REQUEST PAYLOAD TYPE** **GS08 Segment** X12_270_Request_005010X279A1 005010X279A1 X12_276_Request_005010X212 005010X212
SenderIDIllegal	Illegal value provided for SenderID. OR The SenderID in the request does not match the authenticated UserName.	Check that the SenderID value in the request is identical to the SenderID in the Payload.

SenderIDRequired	The field SenderID is required, but was not provided.	Check that the field name is spelled correctly and that a value exists.
TimeStampIllegal	Illegal value provided for TimeStamp.	Check that the valid format of 'yyyy-mm-ddThh:mm:ssZ' is used.
CORERuleVersionRequired	The field CORERuleVersion is required, but was not provided.	Check that the field name is spelled correctly and that a value exists.
VersionMismatch	Illegal value provided for CORERuleVersion.	Correct the value to be '2.2.0' or '4.0.0'

10.4 Appendix D: TMHP Certificate Signature Request Instructions

The purpose of this document is to assist a Submitter in creating a Certificate Signature Request (CSR). The CSR is used to request a TMHP Issued X.509 SSL Certificate. The X.509 SSL Certificate must be used when CORE Operating Rules Version 4.0.0 Safe Harbor connection is used.

Important: You must have Powershell installed

1. Download windows powershell script: http://submittercrl.tmhp.com/tools/submittercsr.ps1
2. Open powershell as administrator
3. Type: & path\to\submittercsr.ps1

   path\to = where script is saved on your computer. Example in red following system Powershell prompt.

   PS C:\Windows\System32\WindowsPowerShell\v1.0> & C:\Temp\submittercsr.ps1

Complete the following entries:

Common Name (enter your server name; e.g. server1.submitter.org):

Organization (e.g. Your Company Ltd):

Organizational Unit (e.g. Your Department -- Billing):

City (e.g. Dallas):

State (e.g. TX):

Country (e.g. US):

Organization Email (e.g. processing@yourcompany.com):

Submitter User Principal Name 1 (this will be your submitter ID); one per line)

Example:

123456789

123456780

Certificate details will be displayed between the BEGIN and END CERTIFICATE REQUEST header and footer.

-----BEGIN NEW CERTIFICATE REQUEST-----

-----END NEW CERTIFICATE REQUEST-----

- Copy CSR to clipboard? (y|n): type 'y' & then <enter>
- Paste copied text in notepad
- Attach and send the .txt file attached to the EDICertificateRequest@tmhp.com email address
- TMHP EDI Helpdesk Analyst will respond via EDICertificateRequest@tmhp.com with an attached .xxx file.
- Accept the .CER Certificate file returned in the EDICertificateRequest@tmhp.com email

Note: Prior to downloading the certificate, change the file extension to .cer

11 Change Log

Ver.	Change	Date
1.0	6.0 Safe Harbor Connection chapter and sections added; including URLs and SOAPUI options.10.0 Appendix C – Safe Harbor Connection chapter and sections added; including Error Codes and Error Messages. Updated Section 4.1 Logon screen.	11/24/2014
1.1	As a part of section 6.0, 7.0 & 9.0/9/1 – inserted the following information regarding real-time connectivity with Texas Medicaid. Note: Real-time is available for Eligibility Verification (270/271), Claims Status and Response (CSI – 276/277) and Prior Authorization Request for Review (278) transaction types. A signed agreement is required prior to submitting real-time transactions. Please contact the EDI Helpdesk to initiate a request to submit real-time transactions. **Note:** *Real-Time submitters who have been approved for Real-Time transactions will follow a different protocol as the environments are different between the FTP Batch submissions and Real-Time submissions. Testing is required, however; Edifecs testing is not required for Real-Time transactions.*	03/12/2015
1.2	Updates for connectivity details to the TIERS eligibility interface through TMHP.	03/01/2017
2.0	Updates related to X12 278 and X12 275 transaction types and new Receiver IDs for Long Term Care PASRR (Preadmission Screening & Resident Review) NFSS (Nursing Facility Specialized Services) form on pages 4 and 6.	06/16/2017
2.2	Updates to sections 6.0, 6.1, 6.1.2, 6.1.3. Pages 12, 13, 14, 15, 16 with regards to Safe Harbor Connectivity under the CAQH CORE version 4.0.0. Page 5, formatted table	06/22/2017
2.3	Updates to sections 6.1.3. Page 15 in regards to SSL Certificate Update. New URL's added under Public Primary Root Certificate and Intermediate Certificate Authority. Added TLS Version to Section 6.1.3 and clients need to use TLS version 1.2	05/06/2018
2.4	Updates to section 10.2, page 23 in regards to the production URL address used with WS_FTP PRO.	03/14/2019

	Updated the URL location used by WS_FTP PRO from 67.67.201.21 to 67.67.201.175.	
2.5	Update to section 4.1.1, updated the URL Location and steps used to install AnyConnect VPN version 4.7	07/03/2019
2.6	Page 3 – Further definition of Texas Medicaid Enrolled and MCO Only Enrolled Providers Page 5 – Added receiver IDs for LTSS – Long Term Services and Support Page 14 – Note added to 2200 REF to indicate that this segment is not populated on encounters transactions.	09/01/2019
2.7	Section 4.2 – Changed the instructions order. Numbers 2 and 3 were out of order. Sections 6.1 and 6.1.2 – Removed all references of IP addresses	08/31/2021