ELECTRONIC DATA INTERCHANGE (EDI)

CONNECTIVITY GUIDE

TMHP
TEXAS MEDICAID & HEALTHCARE PARTNERSHIP
A STATE MEDICAID CONTRACTOR

Table of Contents

1 Introduction 4

Audience 4

2 TMHP Electronic Transactions 5

2.1 EDI Transactions 5

2.2 TMHP Receiver ID Numbers 6

3 Technology Requirements 8

3.1 Secure File Transfer Protocol (SFTP) Requirements 8

3.2 File Compression Techniques 8

4 Secure File Transfer Protocol 9

5 Safe Harbor Connection 10

5.1 Connectivity Standards 10

5.1.1 Hypertext Transfer Protocol/Secure (HTTPS) Multipurpose Internet Mail Extensions (MIME) Multipart 10

5.1.2 Simple Object Access Protocol (SOAP) + Web Service Definition Language (WSDL) 11

5.1.3 SSL Certificates/TLS Version 11

5.1.4 835 File Retrieval via Safe Harbor Connectivity 12

6 TMHP File Naming Conventions 13

6.1 Files Sent To TMHP 13

6.2 Files Sent From TMHP 13

7 Contacting TMHP Electronic Data Interchange Support 14

7.1 Enrollment and Testing Information 14

8 Appendices 16

8.1 Appendix A – SFTP Client Instructions 16

8.1.1 To Upload a File 17

8.1.2 To Download a File 17

8.2 Appendix B – Safe Harbor Connection 18

8.2.1 Connectivity Standards 18
8.2.2 Message Envelope Standards 18
8.2.3 Submitter Authentication Standards 18
8.2.4 Safe Harbor Connectivity 18
8.2.5 Error Reporting 19
8.3 Appendix C: TMHP Certificate Signature Request Instructions 22
9 Change Log 1

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 secure file transfer protocol (SFTP). 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, Texas Integrated Eligibility Redesign System (TIERS) eligibility information is available as an interface through TMHP EDI 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:

1. American National Standards Institute (ANSI) X12N 5010 Implementation Guides which are available on the Washington Publishing Company web site at https://x12.org.
2. The TMHP Companion Guides are available on https://www.tmhp.com/topics/edi.

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 from MCO forwarded claims	ANSI X12 5010	Acute Care
				Long Term Care

Inbound Transaction	Inbound Format	Response	Response Format	Comments
275 Additional Information to Support a Health Care Claim or Encounter	ANSI X12 5010	824 Application Reporting for Insurance	ANSI X12 5010	Attachment for Acute Care Medicare Advantage claims only
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
GS03, Interchange Sender ID	ADVANTAGE This is applicable to Acute Care Medicare Advantage claims only. Utilize the TMHP Production and Test Receiver IDs above in the ISA segment. For claims that are not for Medicare Advantage, use the same values defined for the ISA segment.

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 Acute Care 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 Secure File Transfer Protocol (SFTP) Requirements

TMHP requires SFTP for transferring files and retrieving responses. The user will need an SFTP client program that supports SFTP to connect to the TMHP EDI SFTP server.

3.2 File Compression Techniques

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

4 Secure File Transfer Protocol

The EDI SFTP 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 log on to the EDI SFTP server, the user will need an SFTP client program that supports SFTP. There are many SFTP client programs available either commercially or as internet downloadable shareware (e.g. CuteFTP, WS_FTP Pro, FileZilla, etcetera).

Only secure/encrypted protocols are supported by EDI SFTP. Clients will not be able to connect to EDI SFTP using unsecured (plain) FTP.

The following protocol is supported:

SFTP (SSH File Transfer Protocol) (port 22)

EDI SFTP operates in compliance with FIPS (Federal Information Processing Standard) 140-2 cryptographic modules for all secure protocol interactions as per state and federal cybersecurity requirements issued to Texas Medicaid for secure file transfer. These modules evolve over time as encryption technology evolves and old ciphers are depreciated. Clients using out-of-date or depreciated encryption will be unable to connect to EDI SFTP if the client's program does not support current cryptographic standards.

5 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.

5.1 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 C: TMHP Certificate Signature Request Instructions.

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

5.1.1 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
TIERS Acute Care Eligibility Interface TMHP Receiver ID	617591011TIELT
Test files CORE Envelope version 2.2.0	https://services-uat.tmhp.com/corerules/httpsrequest

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

5.1.2 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
TIERS Acute Care 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
TIERS Acute Care 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 and 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

5.1.3 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:

1. Public Primary Root Certification Authority
   https://certs.godaddy.com/repository/gdroot-g2.crt
2. Intermediate Certification Authority

   gdig2.crt.pem (Privacy Enhanced Mail [PEM]):
   https://certs.godaddy.com/repository/gdig2.crt.pem

   gdig2.crt (Distinguished Encoding Rules [DER]):
   https://certs.godaddy.com/repository/gdig2.crt

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.

5.1.4 835 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 following PayloadType in the response with the 835 attached as the Payload:

   'X12_835_Response_005010X221A1'

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.

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.

6 TMHP File Naming Conventions

6.1 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.

6.2 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:

1. The first 9 digits of the name on downloadable outbound files is the Submitter ID.
2. The second 8 characters are the TMHP assigned alpha numeric Batch ID.
3. 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.

Transaction	File Extension	Description
Prior Authorizations	278	Response to the 278 Request for Review.
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.

7 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.

7.1 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's Test Environment is available to all providers and trading partners.

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.

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 in the TMHP Test Environment.
2. Software vendors that plan to submit transactions to TMHP are required to sign a Trading Partner Agreement and successfully test in the TMHP Test Environment.
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 in the TMHP Test Environment. Clients of these Software Vendors must sign a Trading Partner Agreement.
4. Clearinghouses that plan to submit transactions to TMHP are required to sign a Trading Partner Agreement and successfully test in the TMHP Test Environment.

Note: Real-Time submitters who have been approved for Real-Time transactions will need to follow test for Real-Time submissions in the TMHP Test Environment

8 Appendices

8.1 Appendix A – SFTP Client Instructions

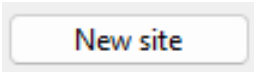
Although TMHP does not require any particular secure file transfer client program, it is highly recommended to use the most recent version of industry-standard secure file transfer programs. Acceptable secure file transfer clients include, but are not limited to, CuteFTP, FileZilla, WS_FTP Pro, etcetera.

Note: The user interface and instructions of your selected SFTP Client may look different than those shown below. Refer to the SFTP client documentation for specific instructions for your chosen SFTP client.

Follow the instructions below to create a new site profile in your chosen SFTP client, or refer to your SFTP client documentation:

1. Open the Site Manager and select the My Sites folder from the list.

Click the **New Site** button.



In the Host Name or IP Address field, type one of the URLs below, depending on need:

Batch	URL
Production	ediSftp.tmhp.com
Regression (Test)	ediSftp-uat.tmhp.com

In the User ID field, enter the current Submitter ID.

In the Password field, enter the assigned Password.

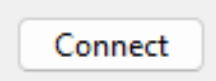
Update the protocol to SFTP if necessary.

You may add or change the name of the site if desired.

Click **OK**. The newly created TMHP site profile will appear in the **My Sites** folder. To make the SFTP connection:

Select the TMHP site name assigned in the **My Sites** folder.

Click the Connect button.



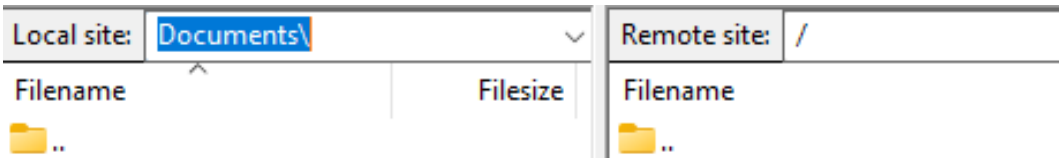
The Site Manager window will close, and the SFTP client will attempt to connect to TMHP EDI SFTP.

8.1.1 To Upload a File

1. Double-click on the **dropbox** folder to open it.
2. Select the file to be uploaded in the Local site pane on the left side of the FTP client, right click, and select Upload.
3. Alternatively, select the file to be uploaded in the Local site pane and drag and drop the file to the folder to upload.
4. When the transfer is complete, a message will appear stating that the transfer is complete.

8.1.2 To Download a File

1. Choose the folder to which the file will be downloaded (the transfer destination). Use the **Local Site** pane of the SFTP client window on the left side of the screen to navigate to the correct folder on your system.



2. Navigate to the download/batch folder on the Remote Site (TMHP EDI SFTP).
3. Drag the file(s) from the Remote Site on the right pane to the destination folder on the Local Site on the left pane.
4. Alternatively, on your system, open the transfer destination folder and drag the file(s) from the Remote Site pane in the SFTP client directly into the transfer destination folder on your system.

The contents of the folder will now be in the selected folder on your system.

8.2 Appendix B – Safe Harbor Connection

8.2.1 Connectivity Standards

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

CORE version 2.2

1. 270/271 Health Care Eligibility Benefit Inquiry and Response
2. 276/277 Health Care Claim Status Request and Response
3. 835 Retrieval of Health Care Claim Payment/Advice

Additional transactions added for CORE 4.0.0

4. 837/277CA Health Care Claim: Institutional
5. 837/277CA Health Care Claim: Professional
6. 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:

8.2.2 Message Envelope Standards

1. HTTP/S MIME Multipart version 1.1
2. SOAP + WSDL version 1.2

8.2.3 Submitter Authentication Standards

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

8.2.4 Safe Harbor Connectivity

1. Conformance to information transportation and message standards, along with response and availability, ensure safe harbor for electronic transactions.
2. 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.

8.2.5 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.)

Error Code	Error Message	Resolution
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.

Error Code	Error Message	Resolution
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'

8.3 Appendix C: 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 **bold** below following system Powershell prompt.

   Powershell prompt - 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-----

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

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

9 Change Log

	Change	Date
1.	Removed references to accessing TMHP EDI SFTP via web browser. Removed references to FTPS. Added FIPS statement. Updated effective date to 5/1/2026. Updated subheading in Section 4 for clarity. Updated URLs in Appendix A.	3/20/2026
2.	Removed Legacy Connectivity Guide.	5/29/2026
3.	Removed prologue indicating EDI changes and go-live date	7/28/2026