CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

Table of Contents

Clicking on each title below will take you to that section.

Revision History

Date	Description of Changes	Version	Author
2/2021	Update reference of EIDM to IDM due to migration.	1.0	CMS
4/27/2021	Merged OIT/ EFT comments; updated Plan Connectivity Milestones and TIBCO connectivity requirements.	1.0	MAPD, OIT, EFT
5/13/2021	Added Gentran Section 6.3.1 and Appendix A.	1.5	MAPD
5/28/2021	Updated document with format changes, QC edits, and verbiage.	1.5	BSS, MAPD
6/11/2021	Updated Document Table and Appendix A. User ID Row added for each connectivity type.	1.5	MAPD
6/18/2021	Updated Gentran section 5.3.1 with additional information. Added Acronym list.	1.5	MAPD
6/24/2021	Final version posted to MAPD Plan Connectivity Preparation page.	2.0	MAPD
6/20/2022	Updated section structure and changes to unify DEPP to Connectivity Checklist.	2.5	MAPD
8/3/2023	Updated Connectivity type table adding in a row about multiple file transfer capabilities.	3.0	MAPD
4/9/2024	Updated MAPD Website URL	3.5	MAPD

Introduction

The purpose of this document is to provide technical instruction to all Medicare Advantage Prescription Drug (MAPD) Plans (referred to in this document as "Plans"), to establish connectivity to the Centers for Medicare & Medicaid Services (CMS). This document focuses primarily on the connectivity needed to submit and receive MAPD Enrollment information and reports. Additional connectivity is required to submit and receive Prescription Drug Event (PDE), Risk Adjustment Processing System (RAPS), and Encounter Data system (EDS) information. See section 4.5 below for information on the PDE, RAPS, and EDS connectivity process.

The scope of this document is to provide information on the following:

1. Get Started
2. Obtain Security and Access
3. Establish Data Transfer Protocols
4. Test Connectivity

This document is intended for Plans that will exchange data with CMS as well as entities that will exchange data on behalf of Plans, such as Third-Party Administrators (TPA).

Please contact the MAPD Help Desk if there are any problems or questions encountered while following the procedures outlined in this document.

MAPD Help Desk:
Phone: 1-800-927-8069
Email: mapdhelp@cms.hhs.gov

Overview

Exchanging information with CMS can be accomplished using different tools and procedures which are dependent on a Plan's current capabilities and the volume of data to be exchanged using one of the following data exchange protocols:

- T1 Connect: Direct
- TIBCO Managed File Transfer (MFT) Internet Server (IS) – Secure File Transfer Protocol (SFTP)/ Hypertext Transfer Protocol Secure (HTTPS)
- TIBCO MFT Platform Server (PS)
- Gentran

1 Get Started

This section will outline the initial steps to begin the process of establishing or updating a Plan's connectivity.

1.1 Obtain a Contract Number from CMS/HPMS

All new Plans participating in the MAPD Program must receive a contract number(s) from CMS or the Health Plan Management System (HPMS) before they can begin. Contract numbers identify the organization and Part D offering, and this identifier typically consists of five (5) alphanumeric characters such as X1234. After obtaining the contract number(s), Plans must register a designated person(s) to enter the Plan's connectivity data into the HPMS Plan Connectivity Data (PCD) Module. For assistance with obtaining a contract number or technical aspects of entering data into the PCD Module, please contact HPMS.

HPMS

- URL: https://hpms.cms.gov.
- This site uses your Resource Access Control Facility (RACF) ID also known as an Enterprise User Administration (EUA) ID to login.
- For RACF/EUA ID assistance, contact CMS IT Help Desk at 1-800-562-1963.
- For Technical assistance with HPMS, contact: hpms@cms.hhs.gov or 1-800-220-2028.

Note: The MAPD Help Desk will monitor new Plan contracts submitted through HPMS and will initiate contact with new Plans to assist in the CMS connectivity process.

For additional assistance, please download the *Technical User's Manual* within HPMS. To download, follow these steps:

1. Log into HPMS.
2. Select 'Contract Management', then 'Plan Connectivity Data.'
3. Select 'Documentation.'
4. Download the *Technical User's Manual.*

1.2 Complete the "Request for Server to Server Access to CMS for Enterprise File Transfer (EFT) Corporate Secure Point of Entry (SPOE) ID" Form

The "Request for Server to Server Access to CMS for Enterprise File Transfer (CMS EFT) Corporate Secure Point of Entry (SPOE) ID" form must be completed and submitted to the Division of Payment Operations Information System Security Officer (DPOISSO).

This form is required for:

- New T1 Connect: Direct connections.
- New TIBCO MFT Internet Server (IS) - SFTP/ HTTPS.
- New TIBCO MFT Platform Server (PS).
- New Gentran setups (required only when automating file transfers).

The link to the Request for SPOE ID form is available in the downloads section of the MAPD Plan Connectivity Preparation page.

Scan and email the completed form to the CMS DPO ISSO at the following email address: DPOISSO@cms.hhs.gov. It is optional but recommended to CC MAPDHelp@cms.hhs.gov.

1.3 Enter Connectivity Data into HPMS Plan Connectivity Data Module

The PCD module will store information on how data will be transmitted and received between CMS and the Plan.

When all contact information and connectivity data is entered into the module, Plans can select the "Create PDF" option to print the completed PCD form. Only one (1) signed form is required if all new contract numbers will use the same data transfer protocol (i.e., T1 Connect: Direct). Otherwise, a separate form will be required for each data transfer protocol. CMS requires a copy of this information, signed by the Plan's External Point of Contact (EPOC) Approver and Organizational Representative, to be scanned and emailed to the MAPD Help Desk before connectivity can be established.

Note: This is the process Plans will use to communicate data routing changes in the future. When the PCD module is updated, Plans need to make sure all TPAs are selected and notified of the change.

Plans that have previously established connectivity to CMS for MAPD Plan exchanges with their existing Plan contract numbers will need to complete the PCD form as well. The PCD form should reference their current configuration. These Plans do not have to complete the activities relating to connectivity set-up and testing. However, they must update the PCD Module in HPMS to add any additional new contracts.

Plans that will use a TPA to submit their Enrollment files must complete additional fields and an additional form within the PCD module. Please review the Technical User Guide within the HPMS website. The additional fields will automatically populate once the "3rd Party" and/or "T1 Connect: Direct" option is selected for Enrollment. After completing all fields on the "Plan Connectivity Data – General" form, select the "Next" button to complete the "Plan Connectivity Data – T1 Connect: Direct/ 3rd Party" form. Users will select from a list of pre-populated TPA organizations. If the TPA organization is not listed, please direct the TPA to the HPMS Help Desk for assistance.

Note: Establishing a new T1 line connection and the associated access can take six (6) to eight (8) weeks to order, schedule, and install. Plans need to take this into consideration if this is the exchange mechanism they plan to use.

2 Obtain Security and Access

To gain access to the Medicare Advantage & Prescription Drug System (MARx), Plan users must possess an IDM account to request a role within the CMS Enterprise Portal. This portal supports three (3) main user roles:

- **External Point of Contact (EPOC)** – Required for connectivity – This role is responsible for approving end-users who are requesting access to CMS systems on behalf of a Plan. The EPOC must have authority from the Plan's organization to authorize user access. Contracts may have more than one user with the EPOC role. **Note:** The EPOC will not have access to the MARx User Interface (UI).

- **MA Submitter** – Required for connectivity – This role is responsible for the transmission/receipt of data files to and from CMS via T1 Connect: Direct, TIBCO MFT IS, TIBCO MFT PS, or Gentran. These users can be resources from a TPA organization[*]. Contracts may have more than one user with the MA Submitter role and each MA Submitter will have access to MARx UI. However, if submitters need to enter and/or update beneficiary enrollment related data through MARx UI, they will also need to request the **MCO Representative UI Update** role.
- **MA Representative** – Optional for connectivity – This role provides access to the MARx UI (called the **MCO Representative** within MARx UI). This role is not required for data exchange but is required for analysis and support of business processes. These users can be resources from a TPA organization[*].

  NOTE: At a minimum, the Plan must have at least one (1) EPOC and one (1) MA Submitter registered to proceed with the connectivity process.

For new users, please see the Enterprise Portal User Guide. For existing IDM Portal accounts, use portal.cms.gov to add your MARx role. For more information on how to register for a role within the CMS Enterprise Portal, please see the MARx EPOC Role Request User Guide and MARx Role Request User Guide which are available in the downloads section of the MAPD Help Desk Website Plan Connectivity Preparation page.

2.1 Submit EPOC Designation Letter to CMS

Before a Plan can register in the CMS Enterprise Portal, they must submit an EPOC Designation Letter with the following requirements:

- Must be on original company letterhead.
- Must contain all the following for each EPOC:
  - name(s) of designated EPOC
  - mailing address
  - telephone number and extension
  - e-mail address
  - contract number(s) for which the EPOC will approve users (list ALL contract numbers)
- Must contain a signature of the responsible officer for the organization.
- Must include the name, title, mailing address, e-mail address, and telephone number of the company official signing the letter.

The link to the template for the letter is available in the downloads section of the MAPD Help Desk Website Plan Connectivity Preparation page.

[*] Assuming Plan EPOC approves the role request.

This form is used to validate and recertify the EPOC's role within the CMS Enterprise Portal and must be done every year. Failure to submit accurate information in this letter will result in no access, or delayed access for all Plan users. Plans are encouraged to identify more than one (1) EPOC, depending on the size of the organization and number of eventual users. This activity should be completed as soon as a contract number is obtained from HPMS. This form will be emailed to DPOEPOC@cms.hhs.gov and MAPDHelp@cms.hhs.gov.

Note: All Plans must submit a letter identifying the EPOCs for each newly assigned contract number even if there is a letter already on file for existing contracts.

2.2 Submit EPOC Access Acknowledgement form to CMS

Within the same email as the EPOC Designation Letter, you will also need to provide a signed copy of the EPOC Access Acknowledgement form for each EPOC request. The link to this form is available in the downloads section of the MAPD Help Desk's Plan Connectivity Preparation page.

This form is used to add, remove, or recertify an EPOC's role(s) on their IDM account within the CMS Enterprise Portal. Failure to submit accurate information on this form will result in the EPOC's access not being approved and will cause a delay in Plan users gaining the needed access.

The EPOC Designation Letter and EPOC Access Acknowledgement Form should be:

- emailed to DPOEPOCS@cms.hhs.gov and copy MAPDHELP@cms.hhs.gov.
- subject line must follow the format below:
    - EPOC name (must match the name used to register in IDM – no nicknames)
    - company Name
    - contract Number(s) – if registering for more than 1, please only enter 1 contract number in subject line
    - example: Subject: Jane Doe, Company Name, HXXXX

2.3 Register EPOC in the CMS Enterprise Portal

Once the forms have been sent and the contract(s) have been loaded in IDM, EPOCs may request the EPOC role within in the CMS Enterprise Portal. New active contracts are loaded into IDM during the first weekend of the month following contract approval in HPMS.

New EPOCs without an existing IDM account will select the "New User Registration" link to complete their registration. They will then select 'Add Application' to verify their identity, request their role, and add Plan contract number(s).

Existing users will enter their user ID and password and select 'Login.' They will then modify their profile to add the new contract numbers. For more information, please see the EPOC Role Request User Guide in the downloads section of the MAPD Help Desk Website Plan Connectivity Preparation page.

NOTE: When registering in the CMS Enterprise Portal, consider the following:

- Potential EPOC users should provide all Plan contract numbers for which they will approve end-users (they may add additional contracts later).
- Enter an e-mail address that is specific to the organization (not a public e-mail such as Yahoo or Hotmail).
- The name used on the EPOC designation letter must match the name used to register in IDM.
- Enter a valid phone number and extension. This information is necessary if an issue arises, and CMS must contact the EPOC directly.

EPOC will receive an email from the CMS Enterprise Portal (donotreply@cms.gov) notifying the user of their role approval.

2.4 Register MA Submitter and MA Representative in the CMS Enterprise Portal

After receiving notification that the EPOC registration for their contract has been approved by CMS, the EPOC may notify the Plan submitters and representatives that they may register in the CMS Enterprise Portal.

As with the EPOCs, new users without an IDM account will select the “New User Registration” link to complete their registration. They will then select ‘Add Application’ to verify their identity, request their role, and add Plan contract number(s).

Existing users will enter their user ID and password and select ‘Login.’ They will then modify their profile to add the new Plan contract numbers. For more information, please see the MARx Role Request User Guide which is available in the downloads section of the MAPD Help Desk Website Plan Connectivity Preparation page.

Once the pending request is approved, the **MA Submitter** or **MA Representative** will receive an email from the CMS Enterprise Portal (donotreply@cms.gov).

Note: Plans cannot establish connectivity without having established at least one (1) MA Submitter in the CMS Enterprise Portal for their new Plan contract number(s).

2.5 Register User/Submitters – PDE, RAPS, & EDPS

All Plans that will exchange Prescription Drug Event (PDE), and/or Risk Adjustment Processing System (RAPS), and/or Encounter Data Processing System (EDPS) data must contact the Customer Service and Support Center (CSSC) Operations Help Desk to complete additional configuration steps.

Phone: 877-534-2722
E-mail: CSSCOperations@PalmettoGBA.com
EDI and Onboarding Connectivity Page:
https://www.csscoperations.com/internet/csscw3.nsf/DID/1S0BTAL9B0

3 Establish Data Transfer Protocols

The following sections describe the requirements to support connectivity and configuration. They describe the options available to the Plans, how to obtain necessary hardware/software, and the configuration and testing required for that option. For a summary of connectivity types, please see Appendix A.

3.1 Large Plan Connectivity (≥ 100,000 in Enrollment; ≥ 10 Gigabyte File Sizes)

Connectivity for large Plans participating in the MAPD program (those with Enrollment of 100,000 or more beneficiaries) should be implemented using a private CMS Wide Area Network (WAN) Ethernet connection and IBM's Connect: Direct software.

3.1.1 T1 Connect: Direct – Existing Connection to CMS

Plans with an established T1 Connect: Direct connection to CMS to transfer enrollment files can follow an abbreviated process. These Plans usually have at least one existing Plan contract number and/or will be using a TPA utilizing T1 Connect: Direct. The abbreviated process includes filling out the PCD module with the existing connection information. This information will include the following:

- User ID and Password
- Mid-Tier Services (mailbox and local node name) or Mainframe (high-level qualifier for production and test, local node name and environment)
- TCP/IP (address and port) or SNA (application ID and SNA net ID)

When returning the PCD Module to MAPDHelp@cms.hhs.gov, please indicate this is an existing connection for your Plan.

Once the Plan has an EPOC and MA Submitter in place, the MAPD Help Desk will send a Service Request (SR) to the EFT Team who will add the new Plan to the existing connection. The EFT Team or the MAPD Help Desk will reach out if there are any questions or concerns.

3.1.2 T1 Connect: Direct – New Connection to CMS

A private CMS WAN Ethernet connection directly connects the Plan to the CMS Network. The software to support the data transfer across the private connection is Connect: Direct, a software product that can be licensed from IBM. Plans are expected to fund the cost of the ethernet connection and software license.

The following form is required for this connection (located in the downloads section of the MAPD Help Desk Website Plan Connectivity Preparation page).

- **Request for Server to Server Access to CMS for Enterprise File Transfer (EFT) Corporate Secure Point of Entry (SPOE) ID** returned to DPOISSO@cms.hhs.gov. It is optional but recommended to CC MAPDHelp@cms.hhs.gov.

For additional information, please contact the MAPD Help Desk.

Plans should ensure that all pages of the **Plan Connectivity Data (PCD) Module** are completed and sent to the MAPD Help Desk prior to establishing connectivity.

The Plan's technical representative or programmer should have the Plan's Job Control Language (JCL) and procedure (aka "PROC") for submitting a file to the CMS mainframe constructed, tested, and ready to be submitted. The following values from this job should be available for confirmation:

1. PNODE (Plan node name)
2. SNODE (CMS supplied node name)
3. SNODEID (CMS supplied SPOE ID (NDM####) and password)
4. Dataset name of file being sent to CMS from the Plan and JCL UNIT value
5. RUNTASK statements and Job name to be submitted after a successful file transfer (CMS supplied)

A CMS technical representative or programmer will have the CMS JCL and PROC for submitting a file to the Plan mainframe constructed, tested, and ready to be submitted. The following values from this job will be available for confirmation:

1. PNODE (CMS node name)
2. SNODE (Plan supplied node name)
3. SNODEID (Plan supplied user id and password, if required)
4. Dataset name of file being sent to the Plan from CMS and JCL UNIT value

3.2 Large and Small Plan Connectivity (see Appendix A) (No Beneficiary Limit; <10 Gigabyte File Sizes)

Two (2) options are available for both large and small Plans:

1. TIBCO MFT Internet Server (SFTP/ HTTPS)
2. TIBCO MFT Platform Server (PS)

3.2.1 TIBCO MFT Internet Server (SFTP/HTTPS)

Organizations opting to use the Secure File Transfer Protocol (SFTP) with the TIBCO MFT Internet Server (IS) will be required to obtain a SPOE ID from CMS and to host a Secure Shell (SSH) server with a Digital Signature Algorithm (DSA) or Rivest-Shamir-Adleman (RSA) public key. See Section 4.2.1 for configuration details.

The following forms are required for this connection (located in the downloads section of the MAPD Plan Connectivity Preparation site):

- **Request for Server to Server Access to CMS for Enterprise File Transfer (EFT) Corporate Secure Point of Entry (SPOE) ID** returned to DPOISSO@cms.hhs.gov. It is optional but recommended to CC the MAPD Help Desk (MAPDHelp@cms.hhs.gov).
- **EFT Partner Server Form** returned to EFT_admin@cms.hhs.gov. It is optional but recommended to CC MAPDHelp@cms.hhs.gov.

For additional information, please contact the MAPD Help Desk.

3.2.2 TIBCO MFT Platform Server (PS)

This option is only for internal connections to the CMS Baltimore Data Center (BDC)/Leidos Managed Data Center (LMDC).

The following form is required for this connection (located in the downloads section of the MAPD Plan Connectivity Preparation site):

> **Request for Server to Server Access to CMS for Enterprise File Transfer (CMS EFT) Corporate Secure Point of Entry (SPOE) ID** returned to DPOISSO@cms.hhs.gov. It is optional but recommended to CC MAPDHelp@cms.hhs.gov. For additional information, please contact the MAPD Help Desk.

3.3 Small Plan Connectivity (<100,000 in Enrollment; <2 Gigabyte File Sizes)

Gentran is an option limited to small Plans because of its file size restriction. With Gentran, Plans have the option to manually submit files (individual IDM User ID required) or to do an automated SFTP pull (SPOE ID required).

3.3.1 Gentran

The Gentran option provides connectivity for small Plans participating in the MAPD program. File size submitted must be less than 2 GB. Gentran servers provide Electronic Data Interchange (EDI) capabilities between CMS and CMS business partners. These servers provide CMS with transaction files from the Plans and provide the Plans with CMS reports.

Gentran is a web-interface that does not require the SPOE ID Request form or EFT Partner server form unless Plans are automating the file processes. Plans are still required to have at least one EPOC and one MA Submitter. Each submitter will be using their individual IDM account on the Gentran website below once the connectivity setup is completed.

Website: https://gis.cms.hhs.gov:3443/mailbox

The following form is *only* required for an automated connection with CMS through Gentran (located in the downloads section of the MAPD Plan Connectivity Preparation site):

- **Request for Server to Server Access to CMS for Enterprise File Transfer (EFT) Corporate Secure Point of Entry (SPOE) ID** returned to DPOISSO@cms.hhs.gov. It is optional but recommended to CC MAPDHelp@cms.hhs.gov.

For additional information, please contact the MAPD Help Desk.

4 Test Connectivity

The following section describes the testing instructions and objectives for large and small Plans.

4.1 Large Plan Testing

Connectivity testing for larger Plans will vary based on whether the connection is new or existing.

4.1.1 T1 Connect: Direct – Existing Connection to CMS

During the connectivity set up process, the Enterprise File Transfer (EFT) Team will send a file through the T1 Connect: Direct set up. They will verify the file was transmitted and received by the Plan. This will conclude the testing of connectivity set up.

MAPD will email the Plan once set up is complete and the test file has transmitted successfully. Once the email is received, Plans will need to make sure mailbox(es) are established and accessible.

4.1.2 T1 Connect: Direct – New Connection to CMS

To test Plan connectivity, the following procedure will be used:

1. A Verizon representative will review and confirm that the T1 line connection is complete and ready for use.
2. CMS will review and confirm that the Plan security access to the CMS mainframe is complete.
3. The Plan's technical representative will review and confirm that CMS' security access to the Plan's mainframe is complete.
4. The Plan's programmer and CMS' programmer will review and confirm the C:D procedures for sending and receiving file values are correct.
5. The Plan's programmer will submit the job to send a file to the CMS mainframe.
6. A MAPD Help Desk Representative will verify that the file transmitted from the Plan mainframe was successfully received at the CMS mainframe.
7. A CMS programmer will submit the job to send a file to the Plan mainframe.
8. The Plan's programmer will verify that the file transmitted from CMS' mainframe was successfully received.
9. A successful test is complete when a file has been sent from the Plan's mainframe to CMS' mainframe and a file has been sent from the CMS mainframe to the Plan's mainframe. The files being sent and received by CMS and the Plan will be empty or contain canned test (not production) data. CMS EFT will work with the Plan to confirm testing was successful.

The *Plan Connectivity Checklist* can be found on the MAPD Help Desk Website in the Downloads section of the Plan Connectivity Preparation page.

4.2 Large and Small Plan Testing

Small Plans should follow the testing procedures defined below for their selected protocol and connectivity methodologies. Section 4.2.1 provides testing information for Plans using the SFTP protocol to the TIBCO MFT Internet Server (IS).

4.2.1 TIBCO MFT IS (SFTP/ HTTPS)

4.2.1.1 SFTP

As indicated earlier, Plans opting to utilize the SFTP protocol with the TIBCO MFT Internet Server will be required to obtain a Secure Point of Entry (SPOE ID) from CMS and host an SSH server with a DSA or RSA public key. If the Plan does not already have a SPOE ID (GIS####), a SPOE ID form must be completed and returned to DPOISSO@cms.hhs.gov. It is optional but recommended to CC MAPDHelp@cms.hhs.gov.

Counter (CTR) Ciphers will not be supported. Only Cipher block chaining (CBC) ciphers are supported as of June 23, 2021.

To send files to CMS, Plans will need an SFTP client that supports Secure Shell Protocol-2 (SSH2) keys. Users will need to generate one of the following:

- An SSH2 RSA 2040-bit key.
- DSA 2040-bit key pair with a passphrase with the SFTP client.
    - For example, Filezilla uses keys generated from PuTTYgen.

To connect, the following configurations must be set in the SFTP client:

- Host name: EFTp2.cms.hhs.gov
- SFTP Port number: 11222 (SFTP traffic from Plan to CMS site)
- SFTP Port number: 11022 or 22 (SFTP traffic from CMS to Plan site)
- Authentication method: key and password
- SPOE ID entered as SYSIDLDAP-GIS####
- RSA SSH2 private key and passphrase
- Compression: zlib (optional)

MFT Internet Server uses both password and key authentication. Please make sure to use your SSH2 key and enable password authentication in your SFTP client.

The CMS Enterprise File Transfer Team (CMS EFT) will provide instructions to upload the public key from this pair to the TIBCO MFT IS. Once the key is enabled in the system, users will be able to connect using the key and the SPOE ID. The CMS EFT Team will aid with sending a test file to confirm connectivity.

To receive files from CMS, Plans will need an SSH server with a DSA or RSA public key. Testing and setup will be coordinated by CMS EFT.

4.2.1.2 HTTPS

Hypertext Transport Protocol Secure (HTTPS) is a secure Web Interface to provide connectivity to the TIBCO MFT Internet Server hosted by CMS. Users will login to the TIBCO MFT Internet Server Web Interface to send data to CMS.

Before connecting to the server through the Web Interface, each Plan will need to configure their network firewalls and Access Control Lists (ACLs) to allow access to the site: https://EFTp2.cms.hhs.gov:11443/.

4.2.2 TIBCO MFT Platform Server (PS)

Testing for this connectivity type will be completed by the CMS EFT Team. For more information, contact the MAPD Help Desk.

4.3 Small Plan Testing

The CMS EFT Team will coordinate testing with the Plans.

4.3.1 Gentran

Testing will include verifying that users can log into Gentran with their individual IDM User ID (users must have the MA Submitter role) or the Plan's Secure Point of Entry (SPOE) ID (GIS####), using this URL:

https://gis.cms.hhs.gov:3443/mailbox/jsp/login.jsp

After logging in, users can verify access to their appropriate mailboxes.

Appendix A – MAPD Plan Connectivity

MAPD Plan Connectivity Summary

Plan Connectivity	Connect: Direct	TIBCO Internet Server (SFTP/ HTTPS)	TIBCO Platform Server (PS)	Gentran
Plan Size	Greater than 100,000 Beneficiaries	No Beneficiary Count Limit[1]	No Beneficiary Count Limit[1]	Less than 100,000 Beneficiaries
File Size Limit[2]	Greater than 10 GB	Less than 10 GB	Less than 10 GB	Less than 2GB
Login ID	SPOE ID	SPOE ID	SPOE ID	IDM User ID, SPOE ID
Multiple File Upload/ Download	√	SFTP only	√	SFTP only
Mailbox Set Up	√	√	√	√
CMS WAN Ethernet Connection	√	n/a	n/a	n/a
Internet Connection	n/a	√	√	√
Software Installation	√	SFTP only	√	n/a
SPOE ID Form Needed	√	√	√	(optional)
EFT Partner Server Form	√	√	√	n/a
Host SSH Server with a DSA or RSA 2048-bit public key	n/a	SFTP only	n/a	n/a
Web Interface hosted by CMS	n/a	HTTPS only	√	√
Automation Possible	√	√	√	(with SPOE ID)
Plans Pull Files	n/a	n/a	√	√
EFT Pushes Files	√	√	√	n/a
Plan Pushes Files	√	√	√	√
File Transfer Status via Email	n/a	By request	n/a	n/a

[1] Although typically used for less than 100,000 beneficiaries, larger Plans can utilize this setup as well.

[2] The number of files is not limited by CMS. The number of records is constrained by the file size limit of the Connectivity type.

Appendix B - Acronyms

List of Acronyms

Acronym	Expanded Definition
ACL	Access Control List
BDC	Baltimore Data Center
CBC	Cipher Block Chaining
CMS	Centers for Medicare & Medicaid Services
CSSC	Customer Service and Support Center
CTR	Counter, an AES block cipher mode
DEPP	Data Exchange Preparation Procedures
DPO	Division of Payment Operations
DPOISSO	Division of Payment Operations Information System Security Officer
DSA	Digital Signature Algorithm
EDI	Electronic Data Interchange
EDPS	Encounter Data Processing System
EDS	Encounter Data System
EFT	Enterprise File Transfer
EPOC	External Point of Contact
EUA	Enterprise User Administration
HPMS	Health Plan Management System
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IDM	Identification Management
IS	Internet Server
ISSO	Information System Security Officer
JCL	Job Control Language
LMDC	Leidos Managed Data Center
MA	Medicare Advantage

Acronym	Expanded Definition
MAPD	Medicare Advantage Prescription Drug
MARx	Medicare Advantage & Prescription Drug System
MCO	Managed Care Organization
MFT	Managed File Transfer
PCD	Plan Connectivity Data
PDE	Prescription Drug Event
PDF	Portable Document Format
PROC	JCL Procedure
PS	Platform Server
RACF	Resource Access Control Facility
RAPS	Risk Adjustment Processing System
RSA	Rivest-Shamir-Adleman
SFTP	Secure File Transfer Protocol
SPOE	Secure Point of Entry
SSH	Secure Shell
SSH2	Secure Shell Protocol
TPA	Third-Party Administrators
WAN	Wide Area Network