Request for Server to Server Access to CMS for Enterprise File Transfer (EFT)
Corporate Secure Point of Entry (SPOE) ID

- Organization Contact* and CMS Approver** must read and sign page 2.
- The CMS Approver must send the completed form to CMS EFT_GTL mailbox

---

1. CMS Application

Service Request number for EFT setup requiring this SPOE ID: _____

CMS Application(s) connected to: _____

---

2. TYPE OF USER ID NEEDED: (Please only check one)

☒ SFTP - MFT Internet Server
☐ Gentran B2BI
☐ MFT Platform Server (CyberFusion)
☐ Connect:Direct (C:D)

3. Organization/Company Information

Organization/Company Name: _____

Organization/Company EIN: _____

Organization Contact Name: _____

Organization Contact Phone: _____

Organization Contact Email: _____

MAPD Plan Contract #/MAC ID: _____

4. Organization/Company Technical Contact Information

Technical Contact Name: _____

Technical Contact Phone: _____

Technical Contact Email: _____

Company Node Name (C:D): _____

---

5. CMS Business Owner Approver Information

CMS Approver Name: _____

CMS Approver Phone: _____

DO NOT WRITE BELOW THIS LINE – FOR CMS USE ONLY

SPOE ID: _____ IDs Assigned By: _____
Tech Contact Notified: _____ Date: _____

SECURITY REQUIREMENTS FOR USERS OF CMS'S COMPUTER SYSTEMS

CMS uses computer systems that contain sensitive information to carry out its mission. Sensitive information is any information, which the loss, misuse, or unauthorized access to, or modification of could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. To ensure the security and privacy of sensitive information in Federal computer systems, the Computer Security Act of 1987 requires agencies to identify sensitive computer systems, conduct computer security training, and develop computer security plans. CMS maintains a system of records for use in assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. CMS records all access to its computer systems and conducts routine reviews for unauthorized access to and/or illegal activity.

Anyone with access to CMS Computer Systems containing sensitive information must abide by the following:

- Do not disclose or lend your IDENTIFICATION NUMBER AND/OR PASSWORD to someone else. They are for your use only and serve as your "electronic signature". This means that you may be held responsible for the consequences of unauthorized or illegal transactions.
- Do not browse or use CMS data files for unauthorized or illegal purposes.
- Do not use CMS data files for private gain or to misrepresent yourself or CMS.
- Do not make any disclosure of CMS data that is not specifically authorized.
- Do not duplicate CMS data files, create subfiles of such records, remove or transmit data unless you have been specifically authorized to do so.
- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.
- Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.
- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including removal from Federal Service, depending upon the seriousness of the offense. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system illegally.

If you become aware of any violation of these security requirements or suspect that your identification number or password may have been used by someone else, immediately report that information to the CMS Service Desk at 410-786-2580 or 1-800-562-1963.

Organization
Contact Signature: _____ Date: _____
(click to digitally sign)

SPOE ID Approvals

CMS Approver Signature: _____ Date: _____
(click to digitally sign)

Instructions for Completing the Request for Access to CMS Enterprise File Transfer (EFT) Secure Point of Entry (SPOE) ID form

This form is to be completed and submitted to request a corporate ID for server to server data transfer to CMS. This ID will be used only to transmit data to and from CMS.
Users transferring files using the Web interface do not use this form and should request an individual SPOE ID on the CMS Portal. https://portal.cms.gov

Questions may be forwarded to the CMS Service Desk at 1-800-562-1963
or email CMS EFT_ADMIN <EFT_ADMIN@cms.hhs.gov>.

1. CMS Application Info – to be completed by the CMS employee sponsoring the data transfer.

Service Request Number:	The Service Request (SR) number to setup the EFT Server to Server Transfer for this SPOE ID. The CMS business owner or GTL must have submitted an SR for EFT to be setup. Creating a SPOE ID without an SR does not provide access to transfer files.
CMS Application(s) connected to:	Name of CMS application(s), such as COBA, MARx or PECOS, that data is being transferred with.

2. Type of User ID Needed: - to be completed by Company
The type of EFT connection the ID will be used for. SPOE IDs are setup differently based on the EFT product being used to transfer files.

3. Organization/Company Information – to be completed by Company

Organization/Company Name:	Name of Organization or company who will transmit data to and from CMS.
Organization/Company EIN:	The organization's or company's Employer Identification Number.
Organization Contact Name:	Individual who serves as contact with CMS.
Organization Contact Phone:	Phone number of contact person.
Organization Contact Email:	Email address of contact person.
MAPD Plan Contract #	For Medicare Advantage Prescription Drug (MAPD) Plans, this is the Plan Contract Number such as H####, S####, etc.
MAC ID	For MAC bank transfers Medicare Administrative Contractor (MAC) ID affiliated with the request.

4. Organization/Company Technical Contact Information – to be completed by Company

Technical Contact Name:	Person who provides technical details and setup for transmittal processing. This person will be contacted with the assigned SPOE ID and connection info.
Technical Contact Phone:	Phone number of technical contact.
Technical Contact Email:	Email address of technical contact.
Company Node Name:	The organization's or company's Connect:Direct/ NDM node name. Leave blank for SFTP, Gentran or Platform Server.

The Organization Contact must read and sign page 2 then forward the signed form to your CMS Contact for approval. Digitally signing and emailing the pdf is preferred.

For Medicare Advantage Prescription Drug (MAPD) Plans, this form should be emailed to the CMS Division of Payment at the following email address: DPOISSO@cms.hhs.gov.

5. CMS Business Owner Approver Information – to be completed by the CMS employee sponsoring the data transfer.

CMS Approver Name:	The CMS business owner who approves the requesting organization should have access to send or receive data with CMS.
CMS Approver Phone:	Phone number of the business owner approver.

The CMS approver is responsible for immediately informing the EFT GTL's of any change in status of the requesting organization.

The CMS Approver must email the electronically signed pdf or scanned signed form to:

CMS EFT_GTL <CMS_EFT_GTL@cms.hhs.gov>