Today’s Date: 10/17/2019 Implementation Date:

|  |  |
| --- | --- |
| **CIGNA Requestor Information: (to be completed by CIGNA)** | |
| Analyst Name: Alexandra Aellano  Analyst Phone: 303-729-8894  Analyst Email: alexandra.arelllano@cigna.com | **Consumer (Check One):**  ☐ ACE/CED  ☐ ACE/CED/CARE ALLIES  ☐ CDH (Webster)  ☐ CBH  ☐ CARE ALLIES  ☐ SELECT - ROUTING834 set to MMS\_Legacy  ☒ SELECT - ROUTING834 set to MMS |
| **Trading Partner Contact Information** | |
| Trading Partner Name : TekPartners  Primary Contact: Lea King  Primary Contact Phone: 515-480-4262  Primary Contact Email: lking@tekpartners.com | Are you an existing Trading Partner  on the Cigna Gateway  If yes , Please provide your Cigna login id cig\_ultimate  Otherwise, fill out pages 3 or 4 for your Transmission Selection.  Secondary Contact:        Secondary Contact Phone:        Secondary Contact Email: |
| **Client Contact Information** | |
| Client Name: Northern Virginia Family Service |  |
| **Additional Information** | |
| File Type: 834/5010  File Schedule: Other (explain :)        File Frequency (specify day of the week and time):        Number of records: | |
| **For 834/5010 Transactions only** | |
| Please provide in the space below the specific data used in the following segments. Note: These fields must be unique between each client/file type (i.e. active file vs. retiree file for same client)  Interchange ID Qualifier (ISA05): ZZ  Interchange Sender ID (ISA06): NORVIRFAMV2V834  Interchange ID Qualifier (ISA07):  Interchange Receiver ID (ISA08):  Application Sender’s Code (GS02): NORVIRFAMV2V834  Interchange Receiver ID (GS03):  Note: Trading Partner Contact will receive a notification from Cigna to initiate the Trading Partner Set-up via [CHCTradingPartnerManagement@Cigna.com](mailto:CHCTradingPartnerManagement@Cigna.com)  If you have any questions please contact your Business Analyst or the Cigna email address:  [CHCTradingPartnerManagement@Cigna.com](mailto:CHCTradingPartnerManagement@Cigna.com) | |

**TRADING PARTNER INSTRUCTIONS**

Cigna offers six (6) types of secure file transfer methods for data exchange.

1. **HTTPS {PGP Optional}**
2. **Applicability Statement 2 – AS2 ─ EDIINT Automated HTTP(s)**
3. **Applicability Statement 3 – AS3 ─ EDIINT FTPS**
4. **FTPS {PGP Optional}**
5. **SSH/SFTP {PGP Optional}**
6. **IBM Connect:Direct w/Secure+**

###### HTTPS {PGP Optional}

* If you have selected HTTPS, please fill out the HTTPS section (**1**) on *Page 3*.
* You will receive a Welcome Package from your Cigna Business Partner. Your Cigna Business Partner will contact you when ready to test. Please do not send data files until your Cigna Business Partner contacts you.

###### AS2 – EDIINT Automated HTTPS

* If you have selected AS2, please fill out the AS2 section (**2**) on *Page 3* with the proper information. Also include your AS2 Certificate and AS2 ID information as an attachment.
* You will receive a Cigna Welcome Package. This will include the Cigna B2B AS2 Certificate and Cigna AS2 ID to upload and setup on your file transfer software. Please do not send data files until Cigna contacts you.

###### AS3 – EDIINT FTPS

* If you have selected AS3, please fill out the AS3 section (**3**) on *Page 3* with the proper information. Also include your AS3 Certificate and AS3 ID information as an attachment.
* You will receive a Cigna Welcome Package. This will include the Cigna B2B AS3 Certificate and Cigna AS3 ID to upload and setup on your file transfer software. Please do not send data files until CIGNA contacts you.

###### FTPS {PGP Optional}

* If you have selected FTP, please fill out the FTP section (**4**) on *Page 3* with the proper information.
* You will receive a Cigna Welcome Package. This will include the Cigna B2B FTP Host address, User ID, and File naming convention with instructions to coordinate testing and set-up.

###### SSH/SFTP {PGP Optional}

* If you have selected SSH/SFTP, please fill out the SFTP section (**5**) on *Page 3* with the proper information. Also include your SFTP server’s SSH Host Key as an attachment.
* You will receive a Cigna Welcome Package. This will include the Cigna B2B SFTP Host address, User ID, and File naming convention with instructions to coordinate testing and set-up.

###### IBM Connect:Direct w/Secure+

* If you have selected Connect: Direct w/Secure+, please fill out the Connect: Direct w/Secure+ section (**6**) on *Page 3* with the proper information.
* You will receive a Cigna Welcome Package. This will include the Cigna B2B Connect: Direct Server Node, IP address, and File naming convention with instructions to coordinate testing and set-up.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TRANSMISSION INFORMATION** | | | | | |
| **Please provide your IP (static or range) and DNS name for inbound connection whitelisting.**  **(only connections from whitelisted sources will be allowed)** | | | | | |
| **Static IP Address:** | ###.###.###.### |  |  |  | |
| **IP Address Range:** | ###.###.###.### | **to** | ###.###.###.### |  | |
| **DNS Name:** | <enter dns name here> | | | | |
| **TRANSMISSION SELECTION** | | | | | |
| **1a.** ☐ **HTTPS 1b.** ☐ **HTTPS w/ PGP**  **2.** **☐ AS2** *HTTP Port: 6080 HTTP(s) Port: 6443 (Please submit your AS2 Certificate w/ EDT Form.)*  Certified AS2 software:  AS2 ID:  HTTP(s) Host/Site name:  URL:    **3.**  **☐ AS3** *FTPS Port: 6021 (Please submit your AS3 Certificate w/ EDT form.)*  Certified AS3 Software:  AS3 ID:  FTP Site Name:       IP Address:  Log-in ID:       *Provide the password via separate email or phone call*  AS3 Message Upload Directory:  AS3 MDN Upload Directory:    **4a. ☐ FTPS** *Port: 6990* **4b. ☐ FTPS w/PGP** *Port: 6990*    **☐ INBOUND: Partner Initiated Put**  **or**  **☐ OUTBOUND: Partner Initiated Get**  **☐ OUTBOUND: Cigna Initiated Put**  **Please fill out the below for Cigna OUTBOUND setups:**  FTP Site Name:       IP Address:  Log-in ID:       *Provide the password via separate email or phone call*  Directory Path, if applicable:  File Name:    **5a.**  **☐ SSH\SFTP** *Port: 22* **5b. ☐ SSH\SFTP w/ PGP** *Port: 22*  **☐ INBOUND: Partner Initiated Put**  **or**  **☐ OUTBOUND: Partner Initiated Get**  **☐ OUTBOUND: Cigna Initiated Put**  **Please fill out the below for Cigna OUTBOUND setups:**  FTP Site Name:       IP Address:  Log-in ID:       *Provide the password via separate email or phone call*  Directory Path, if applicable:  File Name:  **6.** **☐ Connect:Direct w/Secure+** *C:D Standard Port: 1364* | | | | | |

**Roles and Responsibilities:**

**Trading Partner:**

#### **HTTPS {PGP Optional}**

Coordinate testing with your Cigna Business Partner. Also, ensure file transfers are sent using the specified unique filename convention and layout designated.

#### **AS2 (Applicability Statement 2)**

* + For list of Certified B2B Gateway compliant AS2 software, click [here](http://www.drummondgroup.com/html-v2/as2-companies.html).

The Trading Partner’s role is to create an email address specifically for the purpose of this transmission. Send your AS2 Software certificate and maintain annually certificate updates. Also, ensure file transfers are sent using the specified unique filename convention and layout designated.

#### **AS3 (Applicability Statement 3)**

* + For list of Certified B2B Gateway compliant AS3 software, click [here](http://www.drummondgroup.com/html-v2/as3-companies.html).

The Trading Partner’s role is to create an email address specifically for the purpose of this transmission. Send your AS3 Software certificate and maintain annually certificate updates. Also, ensure file transfers are sent using the specified unique filename convention and layout designated.

#### **FTPS** {PGP Optional}

The Trading Partner’s role is to ensure the file is sent using the specified unique filename convention and layout designated.

#### **SSH/SFTP {PGP Optional}**

The Trading Partners role is to send their SFTP servers SSH Host Key if needed. Also, ensure file transfers are sent using the specified unique filename convention and layout designated.

#### **IBM Connect:Direct w/Secure+**

The Trading Partners role is to send their Connect:Direct Server Node and IP information needed. Also, ensure file transfers are sent using the specified unique filename convention and layout designated.

**Cigna Data Movement Services:**

* Cigna Data Movement Services will provide file transfer setup information and details including Cigna Welcome Package.
* Cigna Data Movement Services will contact the Cigna Business and/or Trading Partner regarding any file transfer connectivity testing.
* Cigna Data Movement Services will work with Cigna Business Area to verify, authorize, and approve file transfer for Production status.

**Cigna Business Area/Application Technical Support:**

* Completion of data testing as needed.
* Cigna Business area to follow Cigna standard Systems 2002 Production move-up process if needed.

**Roles and Responsibilities (cont.):**

* Trading Partner communications of actual production date.
* Install host coding changes into production utilizing the Cigna Standard System 2002 Production move-up process if needed.

**Please Note:** These are the Cigna Standard offerings. If these methods cannot be applied, contact our Helpdesk (1-800-810-3388) to schedule a meeting with a Data Movement representative.

If you have a need for a larger file transfer than the listed file size in the Appendix, please contact our Helpdesk (1-800-810-3388) to schedule a meeting with the Data Movement Work Load Coordinator.

**Also Note:** No Shareware or Freeware is supported via Cigna EDI/Data Movement. Shareware and/or Freeware that have known issues with Cigna's EDI network are: *CuteFTP & WinSCP*.

**1. HTTPS {PGP Optional}**

Web browser-based interface that enables partners to upload/download files, subscribe to notifications of events, manage passwords, search and view file transfer activity, and generate reports about file transfer activity.

**Features:**

* Simple Web based Interface
* Secure Access
* Password management
* Transfer Privacy (TLS 1.0 encryption)
* File Transfer Visibility
* Replay/Redeliver
* Notification Subscription
* Individual user log viewing
* Fully monitored service
* Reports
* All file organizations supported

**Requirements:**

* Internet access (TCP/IP)
* Web Browser:

Internet Explorer 6.0 – 11.0 (Windows)

Netscape 7.2 (Windows/MacOS)

Mozilla Firefox 1.4 – 3.6 (Windows/MacOS/Linux)

Safari 1.2 – 4.3 (MacOS/Beta: Windows)

Opera Beta: 9.2 (Windows/MacOS/Linux)

* Only TLS 1.0 Browser Security settings supported
* 2 GB file size limit
* For HTTPS/PGP, you will need a licensed version of the PGP product or any certified PGP compatible application.

**Operating Systems:**

* Any browser based system with internet access

**2. Applicability Statement 2 ─ AS2 ─ EDIINT Automated HTTP or HTTPS**

*HTTP Port:* **6080** *HTTPS Port:* **6443**

AS2 (Applicability Statement 2) is the RFC standard (RFC 4130) by which vendor applications communicate EDI or other B2B data over the Internet using HTTP(s).

**Features:**

* Privacy encrypts a document so only the intended recipient can open it.
* Authentication guarantees that the sender and receiver are who they say they are.
* Integrity confirms that the data sent is the exact data received.
* Non-repudiation uses signed digital receipts to assure that neither party can deny the transaction. The sender receives automated, reliable confirmation of each transaction and/or is alerted if the "signed acknowledgment" is not received within a pre-determined time limit period.  ***Note: certificates must be updated annually.***

**Requirements:**

* Certified AS2 compatible software: See list under test results by clicking [here](http://www.drummondgroup.com/html-v2/as2-companies.html).
* Authorized digital certificate.
* http or https site name for sending file transmission
* Group e-mail box is required for acknowledgements and error notification
* 2 GB file size limit

**3. Applicability Statement 3─ AS3─ EDIINT Automated FTPS**

*FTPS Standard Port:* **6021**

AS3 (Applicability Statement 3) is the specification standard by which vendor applications communicate EDI or other data over the Internet using FTPS.

**Features:**

* Privacy encrypts a document so only the intended recipient can open it.
* Authentication guarantees that the sender and receiver are who they say they are.
* Integrity confirms that the data sent is the exact data received.
* Non-repudiation uses signed digital receipts to assure that neither party can deny the transaction. The sender receives automated, reliable confirmation of each transaction and/or is alerted if the "signed acknowledgment" is not received within a pre-determined time limit period.  ***Note: certificates must be updated annually.***

**Requirements:**

* Certified AS3 compatible software: See list under test results by clicking [here](http://www.drummondgroup.com/html-v2/as3-companies.html).
* Authorized digital certificate.
* FTPS site name for sending file transmission
* Group e-mail box is required for acknowledgements and error notification
* Recommended maximum 15 GB file size limit

**4. FTPS {PGP Optional}** *FTPS Port:* **6990**

**Features:**

* **Inbound: File transfer to Cigna = Partner Initiated Put** – Client uploads the file to CIGNA’s FTPS server.
* **Outbound: File transfer to Customer (Cigna Mailbox) = Partner Initiated Get** – must connect to the Cigna site to download the files.
* **Outbound: File transfer to Customer (Direct) = Cigna Initiated Put** – Cigna uploads the file to client’s FTP site.
* **Optional Encryption** – Pretty Good Protection (PGP) software must be licensed and loaded at the Trading Partner site at their expense.
* Passive and Active mode support.

**Requirements:**

* FTPS capable client.
* External Trading Partner site must have an Internet connection with an Internet Service Provider and be IP enabled.
* Static or Qualified file names are required**.**
* Configuration of multiple IP address at Trading Partners firewall.
* For FTPS with PGP. Pretty Good Protection (PGP) software must be licensed and loaded at the Trading Partner site.
* Recommended maximum 15 GB file size limit
* For FTPS and FTPS with PGP, Only TLS 1.0 is supported.

**5. SSH/SFTP {PGP Optional}** *SFTP Standard Port:* **22**

**Features:**

* Authentication (Password or Key Authentication)
* Privacy (encrypted session)
* Supports both SSH and SSH2
* Standard SSH ports being used

**Requirements:**

* **Inbound: File transfer to Cigna = Partner Initiated Put** – Customer will connect and put files to Cigna’s SSH server.
* **Outbound: File transfer to Customer (Cigna Mailbox) = Partner Initiated Get** – Customer will connect and download files from Cigna's SSH server
* **Outbound: File transfer to Customer (Direct) = Cigna Initiated Put** – Cigna will connect and put files to the client’s SSH server.
* SSH client software must be licensed and loaded at the Trading Partner site at their expense.
* External Trading Partner site must have an Internet connection with an Internet Service Provider and be IP enabled.
* Unique file or qualified file naming conventions are required.
* Open SSH and SECSH Public key format.
* Recommended maximum 15 GB file size limit

**6. IBM Connect:Direct with Secure+** *C:D Standard Port:* **1364**

This is an IBM proprietary file transfer protocol that sends/receives file transfer requests to/from remote Sterling Connect:Direct nodes.

**Features:**

* Authentication (Node Name and IP Checking)
* Privacy (supports Secure+ encryption using TLS)(Required for all internet-based connectivity)
* Retry capabilities for session establishment failures
* Checkpoint/restart capabilities for interrupted file transfers
* Standard C:D ports being used (1364)

**Requirements:**

* Inbound: File transfer to Cigna = Partner Initiated Put – Customer will connect and put files to Cigna’s C:D server.
* Outbound: File transfer to Customer = CIGNA Initiated Put – Cigna will connect and put files to the client’s C:D server.
* IBM Connect:Direct software must be licensed and installed at the Trading Partner site at their expense.
* External Trading Partner site must have an Internet connection with an Internet Service Provider and be IP enabled.
* Unique file or qualified file naming conventions are required.
* Valid CA Certificate for establishing the Secure+ encrypted session using TLS
* Recommended maximum 15 GB file size limit

**Supported Secure+ TLS Cipher Suites:**

* RSA\_WITH\_AES\_256\_CBC\_SHA
* RSA\_WITH\_AES\_128\_CBC\_SHA
* RSA\_WITH\_3DES\_EDE\_CBC\_SHA
* RSA\_WITH\_RC4\_128\_SHA
* RSA\_WITH\_RC4\_128\_MD5

**CIGNA PGP Standards and Details:**

* Cigna supported PGP symmetric Key Algorithms
  + AES (up to 256-bit keys)
  + CAST5
  + TripleDES
  + IDEA
  + Twofish
  + Blowfish
  + Arc4 (128-bit keys)
* Cigna supported PGP Hashes
  + SHA-1, SHA-256, SHA-384, SHA-512
  + MD5
  + RIPEMD-160
  + Public Key Algorithms
  + Diffie-Hellman (up to 4096-bit keys)
  + DSA (1024-bit keys only, verification up to 3072 bits)
  + RSA (up to 4096-bit keys)
* Cigna supported PGP Public Key Algorithms
  + Diffie-Hellman (up to 4096-bit keys)
  + DSA (1024-bit keys only, verification up to 3072 bits)
  + RSA (up to 4096-bit keys)