

Blue Cross and Blue Shield of Illinois, New Mexico, Oklahoma and Texas (BCBS) are pleased to offer Internet FTP. FTP is an industry standard protocol that allows for the transmission of data between systems of varying types using an internet connection. Following are the requirements for utilizing this transmission option:

Requirements:

- FTP client package is necessary, which must include PGP encryption software.
- PGP encryption is MANDATORY. BCBS will not accept unencrypted files and the only method we accept is PGP and GPG. A minimum of 128 bit PGP encryption should be used, however, the higher the bit, the better the protection.
- PGP keys cannot be shared. You must provide ***your*** own public key to HCSC via the FTP Activation Form located in the Electronic Commerce section on the Provider Web site at www.bcbsil.com/provider.
- You must encrypt all files sent to BCBS via FTP using the **HCSC Public Key**.
- You will be assigned a unique BCBS Submitter/Logon ID and password.

Once the FTP Activation Form is submitted to BCBS along with ***your*** Public Key, a BCBS representative will notify you via email when the activation process is completed and when you can begin your Internet FTP transmissions.

Before transmitting Internet FTP files to BCBS, you must download our HCSC Public Key which is located in the Electronic Commerce section on the Provider Web site at www.bcbsil.com/provider.

After you have received your internet FTP confirmation email, the following information will assist you in transmitting files via Internet FTP to BCBS.

The FTP site address is: [ftp.hcsc.net](ftp://ftp.hcsc.net)

- For the Internet FTP logon process, please use your ID number and password (**all uppercase letters**) assigned by BCBS.
- After the logon process is completed, you should find two directories – inbound and outbound.
- All files must be transmitted in binary format – ascii will not be processed. The default setting is ascii; therefore, you must issue the “bin” command to change the format to binary. This change may be confirmed by issuing the “**status**” command and verifying the change was accepted.
- Inbound files to BCBS **MUST** be encrypted with the HCSC Public key. If you do not use the appropriate key, you will immediately receive a decryption error message in your outbound directory.
- Outbound files from BCBS will be encrypted with your public key.

SPECIAL NOTE: Our Legal and Security departments will not allow BCBS to pull files from Client’s FTP servers because it is an added liability to our company. We have no way to guarantee the data is encrypted; therefore, it would be exposed to the internet.

Divisions of Health Care Service Corporation, a Mutual Legal Reserve Company, an Independent Licensee of the Blue Cross and Blue Shield Association.

Inbound File Submission:

To submit the file(s), utilize the “**cd**” command to change to the “**inbound**” directory and enter the following at the FTP prompt:

ftp>put^your transmission file name

Note:

- Each ^ equals one space in the example above.
- The file extension must be **.pgp**, **.gpg**, or **.asc**
- The transmission file name **must not** contain any embedded spaces.
- If you are sending a Cobra file – the file name must begin with “**COBRA**” (all caps).
- If you are sending Self Bill File – the file name **must** begin with “**SELF**” (all caps).
- Wild cards “*” will be accepted only if “**glob**” is on. If you have multiple files to send, you may use the “mput” command, which will prompt you to confirm each file prior to the initiation of each file transfer – unless you have “**prompt**” turned off.

If a problem occurs decrypting the file, an error message file will be generated to your outbound directory in the following format: “Error.2007JAN30.153035” (the date and time stamp displayed will assist you in determining which file BCBS was unable to decrypt). The error response file will contain the following message:

“On 2007-JAN-17 at 13:36:33, inbound file failed decryption. Please call E-Commerce Center at 800-746-4614.”

If you receive this message, there is no need to contact us, please re-encrypt the file with the HCSC Public key and transmit the file again. To ensure you are using the appropriate key, it may be necessary to download the HCSC Public key which is located in the Electronic Commerce section on the Provider Web site at www.bcbsil.com/provider.

Outbound File Retrieval:

After each transmission, utilizing the “**cd outbound**” command, change directories into the outbound directory to see if any messages/responses appear there. If an encryption, translation, or communication problem is encountered with your file a message will be loaded to this directory.

This is the only notification you will receive if the file is not successful, therefore, as a routine part of your process, you should check this directory after each transmission. The “**ls**” command will list all of the files currently available in your mailbox. The file names will vary based on the type of file you receive.

To retrieve the file(s) enter the corresponding file name at the FTP Prompt:

```
ftp>get^RSP####.RSP.INVALID_FILE_HDR
```

Note:

- Each ^ equals one space in the example above.
- The file name you wish to retrieve must match the file name in the outbound directory – exactly (wild cards “*” will be accepted only if “**glob**” is on). If you have multiple files to retrieve, you may use the “mget” command, which will prompt you to confirm each file prior to the initiation of each file transfer unless you have “prompt” turned off.

After a successful download the file is removed from the outbound directory within a few seconds. You should enter the “**quit**” command to end the FTP connection.

Sample outbound file names:

RSP####.RSP.INVALID_FILE_HDR	=	Invalid File Header
RSP####.RSP.REJECTED_ID	=	Login ID and Submitter ID mismatch
RSP####.RSP.ANSI_997	=	ANSI Functional Acknowledgement
MSG####.MSG.INFO_MESSAGE	=	Message-ANSI Translation Error or other informational message
SRG####.SRG.SERGIO.pgp	=	Encrypted Sergio Files
834#####.834.	=	Outbound ANSI X12 Membership Files
Error.2007JUL07.155403	=	Decryption Error File
		(Error.CCYYMonDD.HHMMSS)

The pound signs (#) in the file names above represent numeric values that will vary with each file loaded into the mailbox.

If the file is zipped, the second node of the file name will be “ZIP”.

If the file is encrypted, the last node will be “pgp”.