



HESC's Electronic Data Exchange Systems (EDES)

Sending and receiving data files with HESC using one of our approved transmission methods is cost-effective, safeguarded, and efficient. HESC's EDES will eliminate postage and handling costs, reduce media creation costs, and provide for faster and more efficient updates to our business information systems. Below are brief descriptions of our various Solutions and information on how to get started.

Secured Internet Solution (HTTPS) – “HESC Web File Transfer”

HESC's Web File Transfer process enables our business partners to send and receive files with HESC via an Internet connection and an industry-standard Web browser. Business partners use a unique User ID and Password to log in to HESC's Web site to transfer files--<https://www.hesc.org/webpath/signon.asp>. This method requires a web browser capable of 128-bit encryption and has a file size limit of 30 MB. Files must be in HESC Proprietary or CommonLine format. Also, business partners have the ability to receive (download) their files in Excel format. (Note: No cost to business partners.)

CommonLine SMTP/POP3 (Encrypted E-Mail) -- File Transfer as an encrypted e-mail attachment

HESC's encrypted e-mail process, using SMTP/POP3, enables our business partners to send and receive encrypted files with HESC via e-mail. HESC's encrypted e-mail process currently supports PGP data encryption. This CommonLine File Transfer (e-mail) process has a file size limit of 1 MB for compressed and encrypted files. (Note: Business partners must obtain encryption software.)

NCHELP CAM FTP w/PGP -- “Push-Push Model”

HESC's File Transfer Protocol with PGP process enables our business partners to send and receive CAM (Common Account Maintenance), CL (CommonLine) and HESC Proprietary files with HESC via an Internet server to Internet server configuration. This implements the *Push-Push* model of exchanging files where clients “send/push” files to HESC by placing their files on HESC's FTP server and “receive” files when HESC “puts/pushes” the response files to the client's FTP server. CAM FTP currently supports PGP encryption. All CL and CAM files transmitted with HESC via our CAM FTP method must be named in accordance with the standards outlined by NCHHELP. (Note: Business partners must obtain encryption software, have their own ftp server in order to receive files, and obtain an ftp client to send files. An ftp client may be a PC-, server-, or mainframe-based solution.)

Generic Secure FTP Processes -- “Push-Pull Model” or “Push-Push Model”

Enable business partners with an ftp client or FTP server to send and receive all file types from HESC's FTP server. This implements either the *Push-Pull* or *Push-Push* model. In the *Push-Pull model*, files can be exchanged where clients “send/push” files to HESC by placing their files on HESC's FTP server. HESC places outgoing/response files in the client's “OUT” directory on our FTP server, where the client can then “receive/pull” the files by connecting to the FTP server via their ftp client. In the *Push-Push* model, files can be exchanged where clients “send/push” files to HESC by placing their files on HESC's FTP server and “receive” files when HESC “puts/pushes” the response files to the client's FTP server. For the *Push-Pull and Push-Push* models, files are not required to comply with NCHHELP standards and there are no size limitations.

Encrypted FTP w/PGP -- This method uses an existing Internet connection for the file transfer, but requires the use of PGP software to encrypt data being transferred. (Note: Business partners must obtain encryption software and an ftp client and/or server to send and receive files. An ftp client may be PC-, server-, or mainframe-based.)

For more information, please contact the Data Exchange Team at edes@hesc.org, (518) 408-3685 or Toll Free at 1-866-431-4372 and select option 5.