2. GETTING STARTED – SECURE FILE TRANSFER PROTOCOL (SFTP) PROCEDURES

A. Secure File Transfer Protocol (SFTP) Procedures

Overview

A. IEHP utilizes the Secure File Transfer Protocol (SFTP) server to conduct all electronic data file transactions. Some of the benefits to using the SFTP are:

1. **SFTP is a standard protocol for file transfer**. SFTP is a universally used tool for securely exchanging files between entities.
2. **SFTP provides additional security**. A username and password must be used to establish a connection and data is encrypted during transmission. Each Provider has their own credentials to ensure file transmissions are secure and can be tracked.
3. **SFTP is more flexible**. Files placed on the SFTP server are available until they are picked up. The SFTP server can be accessed twenty-four (24) hours a day, seven (7) days a week. Files remain on the SFTP server for ninety (90) days. They are to be deleted by the submitter. They can be re-accessed multiple times and do not have to be retransmitted.
4. **SFTP complies with HIPAA requirements.** Every file that is transmitted to IEHP is encrypted.

File Transfer Procedures

A. All files for Eligibility, Encounter data, Capitation, and Claims submission must be exchanged via the SFTP using the formats described in:

1. Section 3 - Eligibility Processing Procedures
2. Section 4 - Encounter Processing Procedures
3. Section 5 - Capitation Processing Procedures
4. Section 6 - Claims Processing Procedures

B. The SFTP server can be accessed via a web browser, but there are several graphical user interface (GUI) based SFTP client programs available as well. Examples of these include WS_FTP, FileZilla, and CoreFTP. SFTP functionality may also come bundled into other software products such as Microsoft SSIS and WRQ Reflection. Since the use of an SFTP client varies from vendor to vendor, we are providing instructions for using the internet browser web interface only.

SFTP – Internet Browser Web Interface

A. Open your web browser (e.g. Internet Explorer, Chrome, and Firefox).

2. GETTING STARTED – SECURE FILE TRANSFER PROTOCOL (SFTP) PROCEDURES

A. SFTP Procedures

1. Downloading

B. Navigate to the web address https://sftp.iehp.org/.

C. In the login prompt, enter the SFTP credentials given to you by IEHP, typically based on your Provider ID.

D. Click the Sign On button to view your home screen.

E. Click on the "Folders" link on the left to see home directory. Navigate to the different subfolders used for posting and receiving different types of data files.

F. For some file formats, an OpenPGP standards compatible encryption program like GPG (GNU Privacy Guard) or PGP (Pretty Good Privacy) may be necessary.

***Note**: IEHP may occasionally place messages on the SFTP server that will appear when you log in, please pay attention to these messages.*

Download Files From IEHP – Eligibility

A. From your home directory click the "ELIG" subfolder link.

B. In the "ELIG" subfolder you will find the eligibility file(s) that are ready for download.

C. Click the Download button on the right of the file listing to save it locally.

D. Remember that eligibility files will be encrypted using your public key. An encryption program will be needed to decrypt the files locally using your private key.

Download Files From IEHP – Claims Status Response

A. From your home directory click the "Claims" subfolder link, then from the "Claims" folder list, click the "outbound" subfolder link.

B. In the "outbound" subfolder you will find the claims response file(s) that are ready for download. This will include 999 acknowledgement report files, 277 CA status files, and 835 electronic remittance advice files. To receive 835 files, you must specifically request enrollment.

C. Click the Download button on the right of the file listing to save it locally.

Download Files From IEHP – Capitation

A. From your home directory click the "CAP" subfolder link.

B. In the "CAP" subfolder you will find the Capitation file(s) that are ready for download.

C. Click the Download button on the right of the file listing to save it locally.

2. GETTING STARTED – SECURE FILE TRANSFER PROTOCOL (SFTP) PROCEDURES

A. SFTP Procedures

1. Downloading

D. Remember that capitation files will be encrypted using your public key. An encryption program will be needed to decrypt the files locally using your private key.

2. GETTING STARTED – SECURE FILE TRANSFER PROTOCOL (SFTP) PROCEDURES

A. SFTP Procedures

2. Uploading

Upload Files To IEHP – Encounter Data

A. From your home directory click the "encounter" subfolder link.

B. At the bottom of the screen, use the "Upload a File Now…" function to select which local files to upload.

C. If uploading multiple encounter files, make sure the "Upload files individually" option is selected. This will ensure that files are not grouped into one archive file for upload.

D. Remember, the encounter folder is for the submission of encrypted encounter files only.

Upload Files To IEHP – Claims Submission

A. From your home directory click the "Claims" subfolder link, then from the "Claims" folder list, click the "inbound" subfolder link.

B. At the bottom of the screen, use the "Upload a File Now…" function to select which local files to upload.

C. If uploading multiple files, make sure the "Upload files individually" option is selected. This will ensure that files are not grouped into one archive file for upload.

D. Remember, the claims/inbound folder is for the submission of claims files only.

2. GETTING STARTED – SECURE FILE TRANSFER PROTOCOL (SFTP) PROCEDURES

B. Encryption Questions and Answers

Introduction

A. With some of our transactions, file encryption is utilized to ensure security. IEHP has chosen GNU Privacy Guard (GPG) as our encryption program, but there others also available that take advantage of the OpenPGP standards, like PGP. These are very powerful and fairly easy to use packages that are transportable across several popular platforms. There are many levels of security that can be employed. Both commercial and open source **s**oftware packages based on the OpenPGP Standard can be found. Examples include PGP at http://www.pgp.com/ or GPG at http://www.gnupg.org/.

Installation and Configuration

A. See documentation provided with your software.

Generating Private and Public Keys

A. OpenPGP standard encryption is dual key encryption containing a Private key and a Public key. The Private key is kept secure and will be used to decrypt files received. The Public key is given to the data file sender.

B. The sender uses the Public key to encrypt the data files for transmission. Once the data is encrypted with the Public key, not even the sender can view it. The Private key is now required to decrypt it ensuring that only the intended file recipient will be able to access the data.

C. IEHP will need to receive a Public key from each trading partner. If you do not already have a key pair set up, you will need to generate them. Typically you will need to enter a name, an email address, and a pass phrase (longer then a password) to generate your key pair. Share your Public key with IEHP by emailing it to edi@iehp.org or post it to your home directory on our SFTP.

Decrypting A File

A. Once you have downloaded an encrypted file posted by IEHP, the process of decrypting can vary depending on your encryption software.

1. Typically, you can right click on the file and select the context menu option associated with decryption.

2. Enter the Pass Phrase associated with your Private/Public key set and allow the decrypted file to be saved where you can easily find it.

B. Remember encrypted file extensions may vary. The most common are .pgp, .gpg, and .asc. The extension may have to be configured in your encryption software or changed to suit your software's requirements.

2. GETTING STARTED – SECURE FILE TRANSFER PROTOCOL (SFTP) PROCEDURES

B. Encryption Questions and Answers

Q: What is OpenPGP based encryption software?

A: OpenPGP software allows data trading partners to securely exchange data, relying on Key or Certificate files to encrypt and decrypt the files only by those authorized to do so.

Q: Who needs to have OpenPGP based encryption software?

A: All data Providers: IPAs, Hospitals, Clearinghouses, which exchange data electronically with IEHP may at some point be required to decrypt files posted by IEHP.

Q: Why do we need to have OpenPGP based encryption software?

A: OpenPGP based software allows the users to scramble and encrypt a file. If anyone other than the intended recipient intercepts the encrypted file, it is not readable. PGP also complies with HIPAA and State requirements that a secure means of transmission be implemented.

Q: How do we obtain a copy of an OpenPGP based encryption software?

A: Both commercial and open source **s**oftware packages based on the OpenPGP Standard can be found online. Examples include PGP at http://www.pgp.com/ or GPG at http://www.gnupg.org/.

Q: Can I share my "keys" and if so, how?

A: Yes. Encryption Software based on the OpenPGP standard use key rings or certificate servers to share keys. See your software's guide to find out how.

Q: If different people/entities process Eligibility, Encounter, Capitation, and Claims data for my organization, do I need separate keys/software/etc?

A: While you will not need additional software, it would be best to have different keys for each of these functions to prevent accidental decryption of the various file types by unauthorized personnel.