2. GETTING STARTED

A. Secure File Transfer Protocol Procedures

OVERVIEW:

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

1. **SFTP Is A Standard Protocol For File Transfer**. The SFTP ensures that data is securely transferred using a private and safe data stream. It is the standard data transmission protocol for use with the **SSH2** protocol.
2. **SFTP Provides Additional Security**. A username and password must be used to establish a connection and data encryption is used 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. IEHP Retention time frame is thirty~~ninety~~ (30~~90~~) days for EDI outbound files, after ~~ninety~~ thirty (30~~90~~) day's files will be removed. Inbound files submitted to IEHP via the sFTP will be immediately deleted after being retrieved and archived by IEHP.
4. **SFTP complies with HIPAA requirements.** All inbound and outbound files must be encrypted.

FILE TRANSFER PROCEDURES:

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

1. Section 3 - Eligibility Processing Procedures (834)
2. Section 4 - Encounter Processing Procedures (837I/P)
3. Section 5 - Capitation Processing Procedures
4. Section 6 - EDI Processing Procedures (999, 277CA, 837I/P, 835)
5. Section 19 – IEHP EDI (CCA) (834, 837 I/P, Dental, 999, 277CA)

2. GETTING STARTED

A. Secure File Transfer Protocol Procedures

1. Downloading

A. The Secure File Transfer Protocol (SFTP) server can be accessed via a web browser, but there are several graphical user interfaces (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).

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 the 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 – ENCOUNTER STATUS RESPONSE:

A. From your home directory click the "/5010/Encounters/RESPONSE_PROD/" In the subfolder named RESPONSE_PROD Encounter Submitter's will be able to gain access to IEHP system generated Response Reports.

1. 999 - Functional Acknowledgment
2. 277CA - Claims Acknowledgement Report
3. Encounter Validation Response (EVR)

2. GETTING STARTED

A. Secure File Transfer Protocol Procedures

1. Downloading

DOWNLOAD FILES FROM IEHP – CLAIM REPORTS:

A. From your home directory, go to the following-

Location: /5010/HSP/Outbound

1. TA1- Interchange Acknowledgement
2. 999 - Functional Acknowledgement
3. 277CA - Claims Acknowledgement Report
4. 835 - Electronic Remittance Advice

DOWNLOAD FILES FROM IEHP – CLAIM REPORTS:

B. From your home directory, go to the following-

Location: /5010/CCA/Outbound

1. TA1- Interchange Acknowledgement
2. 999 - Functional Acknowledgement
3. 277CA - Claims Acknowledgement Report

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.

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.

DOWNLOAD FILES FROM IEHP – MISDIRECTED CLAIMS:

A. From your home directory click the "/5010/Misdirect/Outbound/"

1. 837I - Misdirected Claim Files2. 837P - Misdirected Claim Files

B. From your home directory click the "/5010/Misdirect/Images/"
Images - Misdirected Claims Images

2. GETTING STARTED

A. Secure File Transfer Protocol Procedures

2. Uploading

UPLOAD FILES TO IEHP – ENCOUNTER DATA:

Production:

A. From your "home" directory to select the "5010/Encounters/SUBMIT_PROD/ to upload a Production File.

Test:

A. From the "home" directory select the "5010/editest/SUBMIT_TEST/" to upload a Test File.

Encounter Data Manifest:

A. From the "home" directory select the "5010/Reports/Reconciliation Report" to upload your weekly Encounter Data Manifest Reconciliation Report.

UPLOAD FILES TO IEHP – CLAIMS SUBMISSION:

Production:

A. All Medi-Cal and IEHP DualChoice c~~C~~laim s~~S~~ubmissions shall be loaded to the following location 5010/HSP/inbound

~~A.~~B. All Covered California claim submissions shall be loaded to the following location 5010/CCA/inbound

Test:

A. From the "home" directory, select the "5010/HSP/Test/Inbound" to upload a Test File.

~~A.~~B. From the "home" directory, select the "5010/CCA/Test/Inbound" to upload a Test File.

Claims Data Manifest Reconciliation Report:

A. From the "home" directory select the "5010/Manifest/Inbound" to upload your daily ~~——~~Claims Data Manifest Reconciliation Report.

UPLOAD FILES TO IEHP – MISDIRECTED REPONSE FILES:

Production:

A. All Misdirected Response files shall be loaded to the following location 5010/Misdirect/Inbound

Test:

From the "home" directory, select the "5010/Misdirect/Test/Inbound" to upload a Test File.

2. GETTING STARTED

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 software 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: Do I need a separate encryption key for my organization for various file types?

A: No, separate encryption keys for various file types are not required. One encryption key can be used to encrypt and decrypt all file types.

Q: What file types require encryption?

A: All data transmitted to IEHP or out bounded by IEHP that contains Protected Health Information (PHI) and Personally Identifiable Information (PII) require encryption.