

## **Section I**

### **Transmission Modes**

<b>Transmission Options Available.....</b>	<b>2</b>
E-mail Attachment .....	2
Value Added Networks (VAN) .....	2
File Transfer Protocol (FTP).....	2
<b>Sending Data as an E-Mail Attachment.....</b>	<b>3</b>
More on Digital Certificates .....	5
Tips on using E-mail Transmission.....	5
<b>Storing and Receiving Data with File Transfer Protocol.....</b>	<b>6</b>
FTP Name and Internet Address.....	7
FTP Server Account and Password .....	7
Polling Processes .....	7
FTP File Conventions .....	7
<b>Transmission Pathways.....</b>	<b>8</b>

## Transmission Options Available

There are three options available to claims administrators for transmitting data to the WCIS:

### E-mail Attachment

The WCIS can receive data as an e-mail attachment using the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol. Both e-mail messages and attachments will be confidential through authentication and encryption, using digital certification. For more information, see “Sending Data as an E-Mail Attachment” in this section.

### Value Added Networks (VAN)

A Value Added Network (VAN) is a commercially-owned network that provides specific services, such as access to a specialized database for a fee, which is restricted to users. Organizations that provide VAN services act as intermediaries during electronic message exchange. VAN customers typically purchase leased lines that connect them to the network or use a dial-up number, given by the network owner, to gain access to the network.

The advantages of using a VAN include security, auditing, and tracking capabilities, and in some cases, formatting services.

Several EDI service providers provide VAN services. Be aware that billing can be complex, and it typically consists of per byte charges and per “envelope” charges, which vary depending on how the user sends the information. Note: the Division of Workers’ Compensation does not pay VAN charges for either incoming or outgoing EDI transmissions. VAN messages will not be transmitted if the trading partner does not specify that it will accept charges for both incoming and outgoing transmissions. See Section J—EDI Service Providers, for VAN contact information.

### File Transfer Protocol (FTP)

WCIS will poll trading partner File Transfer Protocol (FTP) servers to receive and send data. The internet file transfer protocol is defined in RFC 959 by the Internet Engineering Task Force and the Internet Engineering Steering Group. Data files will be confidential by using Pretty Good Privacy (PGP) authentication and encryption. A history of the PGP program and frequently asked questions is available at <http://www.pgpi.org>.

Trading partners must provide a secure FTP server that is accessible by WCIS. WCIS will only pull data and push acknowledgement to trading partner FTP servers. For more information, see “Storing and Receiving Data with File Transfer Protocol” in this section.

## **Sending Data as an E-Mail Attachment**

Your e-mail software must comply with the Secure/Multipurpose Internet Mail Extensions (S/MIME) format to send secure e-mail to WCIS. Please check with your system administrator to ensure that your e-mail software is S/MIME compliant before proceeding with the following steps. Trading Partners that are unable to send S/MIME e-mail may send files encrypted by Pretty Good Privacy (PGP) to: [wcispgp@dir.ca.gov](mailto:wcispgp@dir.ca.gov). Please contact your Trading Partner liaison for instructions on how to send PGP encrypted files.

This section should be read in conjunction with Section G—Test, Pilot, Parallel, and Production Phases of EDI.

### **Step 1. Trading Partner Profile**

Complete the Trading Partner Profile form as instructed in Step 1 of Section G. Be sure to indicate that the transmission mode is e-mail attachment. Also include the e-mail address where the acknowledgments will be returned. The return address does not need to be the same as the sending address. After the Trading Partner Profile form is completed, follow the steps below. Upon completion of the below steps, return to Section G, Step 2: Complete the Test Phase.

### **Step 2 . Purchase a Digital Certificate**

Purchase a digital certificate from one of the state-certified vendors. The approved list of Digital Signature Certification Authorities is available at the Secretary of State website (<http://www.ss.ca.gov/digsig/cert1.htm>). The digital certificate will authenticate the data you will be sending to us.

### **Step 3. Install the Digital Certificate**

The digital certificate can be installed either from a software disk or directly from the internet. The digital certificate will be installed in your e-mail program and on your internet web browser (e.g., Microsoft Internet Explorer, Netscape Navigator). Details for installation of digital certificates are available at the website of the specific Digital Signature Certificate Authority you choose to purchase from.

### **Step 4. Exchange Digital Certificates with WCIS**

The exchange of digital certificates is necessary for authentication and encryption. The Trading Partner sends WCIS their digital certificate so that WCIS can ensure that the message has not been altered by someone else. WCIS sends the Trading Partner its digital certificate so that the Trading Partner

can encrypt the e-mails sent to WCIS. Encryption ensures that the message and its attachments are not readable by anyone other than the intended recipients.

To exchange digital certificates, send a digitally signed e-mail message to [wcisdata@dir.ca.gov](mailto:wcisdata@dir.ca.gov) with the subject header "REQUEST PUBLIC KEY". Details for sending a digitally signed e-mail are available at the website of the specific Certified Digital Signature Authority you choose to purchase from. Upon receipt of a signed e-mail message, WCIS will respond with a digitally signed message.

The digitally signed e-mail message contains a copy of the WCIS digital certificate. The trading partner must register the WCIS digital certificate with their e-mail system. See your system administrator or the help files of your e-mail program for complete instructions on registering the WCIS certificate on your machine.

If a Trading Partner does not receive a digitally signed e-mail message from WCIS, they should notify their WCIS Contact Person.

### **Step 5. Set Up Your E-mail Program to Encrypt all Data Transmissions to WCIS**

Once digital certificates have been exchanged between users, e-mail messages can be encrypted and signed to protect against tampering. Encrypting a message means you "scramble" the message and its attachment so that only the intended recipient can read it. All messages sent to [wcisdata@dir.ca.gov](mailto:wcisdata@dir.ca.gov) must be encrypted and signed. If a message is received that is not encrypted, the Trading Partner will be notified either by e-mail or by the WCIS contact person. If messages continue to be received un-encrypted, a Trading Partner may not be allowed to use the email facility to send their data. Details for configuring the encryption of a digital certificate message are available at the website of the specific Digital Signature Certification Authority you choose to purchase from.

### **Step 6. Send your Transmissions**

Send an EDI test file, as specified in Section G Step 2: Complete the Test Phase. To send the test file: format the file, attach the formatted file to an e-mail message, encrypt the message, sign the message, and send to [wcisdata@dir.ca.gov](mailto:wcisdata@dir.ca.gov). Data file names should be unique. The subject line should read "SEND EDI DATA".

If transmission of the encrypted and signed test file from a trading partner is successful, WCIS will process your transmission and return a header level acknowledgment to the e-mail address provided on your Trading Partner Profile. E-mail acknowledgments will be returned in the same file format as the original transmission. E-mail acknowledgments will not be encrypted or signed. See Section G for further information on completing the Test, Pilot, Parallel and Production Phases.

## More on Digital Certificates

Digital certificates bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information. A digital certificate makes it possible to verify someone's claim that they have the right to use a given key and helps to prevent people from using fictitious keys to impersonate other users. Used in conjunction with encryption, digital certificates provide a more complete security solution that authenticates the identity of all parties involved in a transaction.

In order to send and receive secure e-mail using a digital certificate, you must be working with an e-mail software that supports S/MIME, the standard format that allows users with different e-mail software to communicate with one another.

## Tips on using E-mail Transmission

- Always encrypt and digitally sign e-mail messages when sending to WCIS.
- Keep the digital certificate current. If a digital certificate has expired, WCIS may not receive your transmission.
- Make sure that your email address matches the email address on your digital certificate. Sometimes the email address you use is different from what is maintained by your email system.
- Do not send any other type of messages to [wcisdata@dir.ca.gov](mailto:wcisdata@dir.ca.gov). The wcisdata mailbox is for EDI transmissions only. All other messages will be deleted and not read.
- Acknowledgements are sent back from [ediout@dir.ca.gov](mailto:ediout@dir.ca.gov).
- The Acknowledgement is an email attachment with the file extension "txt.snd". The Acknowledgement file can be read by removing the "snd" extension, so that the filename should be "*filename.txt*".
- Use unique filenames for each EDI file.

## **Storing and Receiving Data with File Transfer Protocol**

Certain processes and procedures must be coordinated to ensure the efficient transmission of data and acknowledgement files via FTP.

### **Step 1. Trading Partner Profile**

Complete the Trading Partner Profile form as instructed in Step 1 of Section G. Be sure to indicate that the transmission mode is Internet File Transfer. Acknowledgments will be returned by FTP or email. After the Trading Partner Profile form is completed, follow the steps below. Upon completion of the below steps, return to Section G, Step 2: Complete the Test Phase.

### **Step 2. Generate a Pretty Good Privacy (PGP) Key**

WCIS uses PGP to for encryption and authentication. PGP is an encryption program available from PGP Corporation (<http://www.pgp.com>) and the International PGP home page (<http://www.pgpi.org>). PGP is also available from previous versions of security programs offered by Network Associates (<http://www.nai.com>), which had previously acquired the license to distribute PGP.

If the Trading Partner does not already have a PGP key, it will need to generate its own unique set of PGP keys. The PGP program will create a set of public and private keys based on information you enter into the program.

### **Step 3. Exchange PGP Public Keys**

The PGP public keys are required for encryption to provide data security. Data sent to WCIS is encrypted by WCIS's public key and files are signed by the Trading Partner's private key. The exchange of public keys ensures that the recipient is the only one that is able to read the file and that the sender is the only one that could have sent the data. Please do not share private keys and passwords with anyone else as this would allow others to create files that would appear to have come from you.

E-mail your PGP public key to your EDI contact person. Your contact person will send you a copy of the WCIS PGP public key. Exchange of PGP keys is based on mutual trust between WCIS and Trading Partners.

#### **Step 4. Import WCIS PGP Public Key**

Import the WCIS public key into the PGP program. Implicitly trusting the key will facilitate communications without the inconvenience of having to verify the key each time it is used.

#### **FTP Name and Internet Address**

The FTP server must have a static network internet address. The FTP server must be accessible either by a Uniform Resource Locator (URL) (e.g.; <ftp.tradingpartner.com>) or an internet address (e.g.; 10.10.10.10). Enter the network internet address information on C3 on the Trading Partner Profile form. If the address of the FTP server changes, please contact your trading partner liaison to update your Trading Partner profile information.

#### **FTP Server Account and Password**

WCIS requires an account and password on your FTP server. The account and password is entered in C4 on the Trading Partner Profile form. Make sure that it is set and does not change. If the account and password is changed, please update your trading partner profile information.

#### **Polling Processes**

WCIS will periodically poll trading partner FTP servers. An FTP client program will log onto the trading partner server and it will download all files in a directory named inbox on the FTP server. After all the files are retrieved, the client program will delete all files in the directory on the FTP server. Files received will be unencrypted by WCIS with its private key and the trading partner's digital signature will be verified.

WCIS will send acknowledgment files to trading partners, either by FTP or email. Files that are sent by email will be sent to the trading partner's email address, which is listed in C3 of the Trading Partner Profile form. If the email address is blank on the form, acknowledgements will be placed into a directory named Outbox on the FTP server.

#### **FTP File Conventions**

Files should follow these conventions:

- Data files should contain no more than 1,500 FROI or SROI transactions.
- Data file names must be unique and start with 3 letters assigned by WCIS.
- Data files must be encrypted with PGP and signed.
- Acknowledgement files will be unique.
- Acknowledgement files will not be encrypted.

## Transmission Pathways

