



California HIV/AIDS Surveillance
Standard Operating Procedures

External

How to Use the Secure File
Transfer Protocol (SFTP) Network

Version 4.6

January 17, 2012

Standard Operating Procedures

REVISION HISTORY

Version #	Revision Date	Summary of Changes	Revised By
1.0	02/22/2011	Initial draft	Gary Horpedahl
1.5	02/23/2011	First Revision	Gary Horpedahl
2.0	02/25/2011	Second Revision	Gary Horpedahl
2.5	02/25/2011	Made minor wording changes	Steven Starr
3.0	02/28/2011	Technical Review and Revision	Victor Borromeo
3.5	04/18/2011	Addition: Renaming file	Gary Horpedahl
4.0	08/17/2011	Minor process updates	Gary Horpedahl
4.5	11/09/2011	Update naming conventions for files	Gary Horpedahl
4.6	1/17/2012	Update SFT address.	Gary Horpedahl

Standard Operating Procedures

All California LHJs have established accounts on a secured server so each jurisdiction can use the Secure File Transfer Protocol (SFTP) for retrieving and sending confidential data with the Office of AIDS Surveillance section. This process eliminates the more expensive and less timely use of traceable mail used for transmission of DUA datasets, case checks, and lab data reports.

By default, all data is encrypted when uploaded to the server, and decrypted when downloaded from the server. However, as an additional security precaution, OA requires that all files containing confidential information uploaded to the SFTP site be encrypted using OA's SealEncrypt 4.1, PGP, or WinZip version 9 or later.

NOTE: Once an LHJ takes its data off the secured server, the data must be placed in a secured environment. Any CD or flash drive used to transfer the data must be destroyed and/or wiped clean. LHJs are responsible for the ongoing security of the data.

Steps for using the SFTP:

- Initially, LHJs contact their Surveillance Processors and let them know that their county is ready to use the SFTP site, meaning they have lab data to send from the LDET, case checks to run, or quarterly DUA dataset to retrieve.
- The Surveillance Processor secures the Login ID and Password and the link to the SFTP web site and sends it to the LHJ.

Receiving Data

When data for an LHJ is placed on the server by OA (quarterly DUA dataset, case check response), the LHJ Surveillance Coordinator receives an email notification that the data is there.

- The LHJ logs in to the secure server, <https://sft.ca.gov/> using the Login ID and Password assigned to it.
 - Select the file to download and click on it to open the File Download screen; select the download location.
 - Transfer the file to a CD or flash drive so the data can be transferred to your stand-alone secured computer or a secured location.
 - Upload the data file to your stand-alone computer or a secured location.
 - Decrypt the data file using the correct decryption tool (SealEncrypt, PGP, or WinZip). **If using SealEncrypt, the decryption process requires the renaming of the file to “transfer.zc.”**
- Delete the information from the CD or flash drive, or destroy the CD if it is “read only”.
- Once the data is secured, the LHJ deletes the data from the SFTP server by clicking on the File Options icon under File Options, choosing delete, and logs off.

Standard Operating Procedures

Sending Data

When sending confidential data to OA (LDET data, case check requests, etc.), LHJ encrypts and uploads file to the SFTP server.

- LHJ logs in to the secured server, <https://sft.ca.gov>, using the Login ID and Password assigned to it.
- Click on the Browse button to locate the file you want to upload
- **(Please use the following naming conventions to rename the file:**

Name of county_type of file_initials_date_time_transfer.zc

Examples: Sonoma_cc_kg_110411_220_transfer.zc tells OA:

Sonoma County submitted a file for case checks (cc) from Karen Gordon (kg) on November 4, 2011 at 2:20.

Current file types most commonly used are:

Case Checks = cc

Labs

Match Project = match

- Click on the Upload File button to upload your file.
- Log off the SFTP web site
- Send an email to the person at OA who you want to get your data, stating that you have put data on the SFTP server, and the name of the file.
- OA receives an automated message that a new file was uploaded to the system
- The staff person at OA to whom you sent the email retrieves the file and deletes it from the SFTP server.