Sending Sensitive Information to CIVHC

The Center for Improving Value in Health Care (CIVHC) strictly adheres to state and federal laws for data protection. This includes requirements under the Health Information Portability and Accountability Act (HIPAA) for safeguarding Protected Health Information (PHI) and Personally Identifiable Information (PII) such as patient names, dates of birth, and demographic information, among many others.

CIVHC cannot accept any sensitive or protected information via email under any circumstances. If your project requires transferring sensitive information to CIVHC, you will be asked to submit these files to our secure Data Enclave via Secure File Transfer Protocol (SFTP). This guide will walk you through creating an account and uploading your file(s). Your CIVHC contact can help you through this process; please reach out for help if needed!

How the Secure Upload Works

CIVHC maintains a secure remote server (Data Enclave) where analysts perform their work. This environment does not have an open internet connection, and the only way to move data in or out is through SFTP. You will perform these steps to transfer your data to CIVHC:

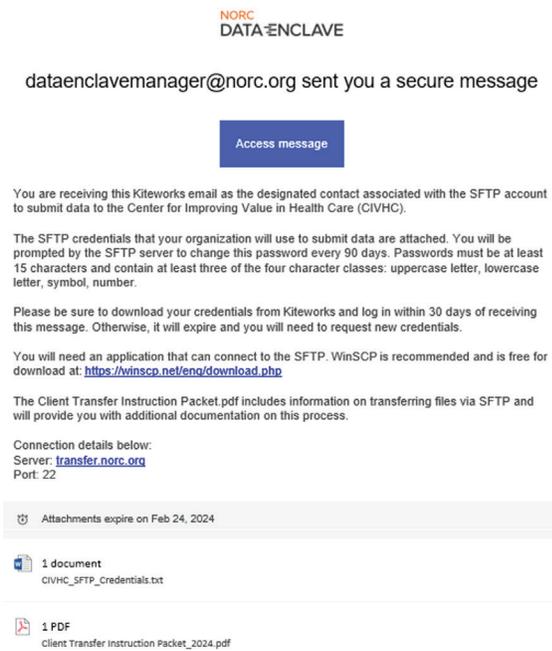| Step 1:	Step 2:	Step 3:
Create and access an Accellion Kiteworks Portal account	Encrypt your data file	Send your encrypted file via SFTP (note: SFTP client software required)

Step 1: Create and Access Your Account

1. Review, sign, and return via DocuSign the Secure File Transfer Protocol Form for Document Upload sent by CIVHC. The contact's name and email address must be for the individual who will perform the upload.

2. The specified individual will receive two emails from the Data Enclave Managers at NORC.

   a. The first email, from dataenclavemanagers@NORC.org, will include an SFTP Username. Save this to connect to the SFTP server.

   b. The second email from NORC will be a secure message notification with a link to a secure messaging portal **(Kiteworks)**. This message is specific to your email address and cannot be forwarded.

      I. Click "Access Message."

      II. Enter your email address (must match the one used to create your account).

      III. On your first visit to the portal, you will be prompted to create a password. Keep this in case you need to log back into the portal later.

      IV. NORC sends your SFTP password through this portal. Open the message in your portal Inbox to access the attached file with your SFTP Password. Do NOT use this portal to send data to CIVHC.

NORC
DATA ENCLAVE

dataenclavemanager@norc.org sent you a secure message

[Access message]

You are receiving this Kiteworks email as the designated contact associated with the SFTP account to submit data to the Center for Improving Value in Health Care (CIVHC).

The SFTP credentials that your organization will use to submit data are attached. You will be prompted by the SFTP server to change this password every 90 days. Passwords must be at least 15 characters and contain at least three of the four character classes: uppercase letter, lowercase letter, symbol, number.

Please be sure to download your credentials from Kiteworks and log in within 30 days of receiving this message. Otherwise, it will expire and you will need to request new credentials.

You will need an application that can connect to the SFTP. WinSCP is recommended and is free for download at: https://winscp.net/eng/download.php

The Client Transfer Instruction Packet.pdf includes information on transferring files via SFTP and will provide you with additional documentation on this process.

Connection details below:
Server: transfer.norc.org
Port: 22

⏱ Attachments expire on Feb 24, 2024

📄 1 document
CIVHC_SFTP_Credentials.txt

📄 1 PDF
Client Transfer Instruction Packet_2024.pdf

The secure email message will look something like this.

Step 2: Format and Encrypt Your Data File(s)

1. Format and name your file(s) according to the Client File Transfer Instruction Packet **(Element Specifications, page 2)**. The file name must include the project number sent by your primary CIVHC contact.

2. Encrypt your file(s) and send the password to your primary CIVHC contact (this can be emailed). See the Client File Transfer Instruction Packet **(Encryption Instructions, page 8)** for detailed instructions.

Formatting Requirements

File Name: Include CIVHC Project Number **(##.###_Finder File)**

File Type: A pipe-delimited text file is optimal **(Field1|Field2|Field3…)**

Match Elements:

  Unique ID: (client-specified, any format)

  Social Security Number: 9-digits, no dashes **(111111111)**

  Medicaid ID: One Letter followed by 7 digits, no spaces or dashes **(A1111111)**

  First Name: No Punctuation **(AAAAA instead of A'AAAA)**

  Last Name: No Punctuation **(OBrian instead of O'Brian)**

  Date of Birth: MM-DD-YYYY, include leading zeroes **(09-19-1999)**

Step 3: Sent Your Encrypted File(s) via SFTP

1. If you do not have SFTP client software, or if you are unsure, contact your IT Department for assistance. The Client File Transfer Instruction Packet **(What is a SFTP Client?, pg.1)** also includes a link to download one option, WinSCP.

2. Open your SFTP Client and connect to the CIVHC server **(Client File Transfer Instruction Packet, page 4).**

3. Move your encrypted file(s) to "Incoming"
   – this is your upload step.

4. Disconnect from the server.

5. Email your primary CIVHC contact to let them know your transfer is complete. They will confirm that your transfer was received.

SFTP Connection Details

- **Server:** transfer.norc.org

- **Port:** 22

- **Username:** SFTP Username

- **Password:** SFTP Password

CIVHC
CENTER FOR IMPROVING
VALUE IN HEALTH CARE

civhc.org   720-583-2095   info@civhc.org   4500 Cherry Creek Dr South Ste. 350, Denver, CO 80246