

Assessment of Chemical Exposures (ACE) Investigations

Manual of Procedures

January 12, 2021
Version 0.1.1

Agency for Toxic Substances and Disease Registry
Centers for Disease Control and Prevention
4770 Buford Highway
Chamblee, GA 30341



Publication History

Author	Date	Version	Reason for Change
Brian Nicholson	1/8/2021	0.1	Initial draft document. Revised Camp Lejeune Cancer Incidence Study for use with ACE investigations.
Maureen Orr	1/12/2021	0.1.1	Changes made
Brian Nicholson	1/14/2021	1.0	Responded to Maureen's comments. Revised sections and added new comments.

Contents

Introduction.....	4
Brief Overview of the Study.....	4
Continuous Maintenance of Staff.....	5
Rules of Behavior.....	5
Out-Processing of Staff.....	6
Notification.....	6
User System Access.....	6
Return of Equipment.....	6
Procedures for Requesting Access to Data.....	6
Encrypted Multi-User Share Tool (MUST) Share.....	6
File Level Encryption.....	9
Client Whole Disk Encryption.....	9
Requests to Move PII from Encrypted Share.....	9
Securely Receiving/Sending Data.....	10
Data Disclosures.....	10
Transfer of data.....	11
De-identification of Data.....	13
Privacy.....	13
Setting up Encryption Software – Local Laptop Folders and Share.....	13
Symantec Encryption (PGP) Software Install Additional Help.....	13
How to Test Encryption on Local Laptops.....	15
Shredding of Electronic Files Using Encryption.....	15
Incident Response.....	16
Email Usage and Web Browsing.....	16
References/Associated Documents.....	17

Introduction

This Manual of Procedures (MOP) is a guidance document that details this study's conduct and operations as well as facilitates consistency in data management practices across users of the data. It is a guideline document that describes the data handling for the study and how it is to be executed. The MOP is provided to each member of the Study Team. The MOP contains an adequate amount of detail that study staff and contractors could process PII data consistently with only the information contained in the MOP and its appendices.

Brief Overview of the Study

- Data will be collected on people who were in the area of the environmental incident so that we can determine the extent of injuries and the immediate needs of the exposed. Data are collected using modifiable forms and other materials in the ACE toolkit. Usually it takes a few weeks for the health department to decide to contact us for assistance. However, there may be the need for a more urgent data collection while the incident is still active or immediately thereafter. Generally the Epi CASE form will be used in those situations. It is important to note the Epi CASE form in the toolkit has the potential to collect sensitive PII, including up to 9 digits of the social security number.

Role Definition

- The ACE Epi-Aid investigation lead will be determined at the time of the request. They will be either a CDC Epidemic Intelligence Service Officer (EISO) or a Career Epidemiology Field Officer (CEFO). There will be other EISO or CEFO who support the lead.
- Surveillance Team Lead Maureen Orr
- ACE ATSDR Program Lead: Stacey Konkle
- ATSDR and NCEH staff will provide technical guidance. At least one staff member will accompany the team in the field at all times
- Additional ATSDR and NCEH staff in Atlanta will provide technical support remotely such as mapping of the exposure, subject matter experts for the substance released, etc.
- The requesting agency (state or local health department) will provide volunteers to help the Epi-aid team.

Onboarding of Staff

All staff that will work with PII will need to sign the following before beginning work on the study:

- Non-Disclosure Agreement
- Study Specific Rules of Behavior

Both documents will be provided to the data steward for secure storage in the *Raw Data* folder of the encrypted Multi-User Share Tool (MUST) share.

Additional if contractors are hired to assist in the data collection they must also complete

People Processing (<https://peopleprocessing.cdc.gov/>)

- Forms needed: People Processing Intake Profile, E-QIP, New User form (<http://itsotools.cdc.gov/csb/newuser.aspx>)
- Trainings required:
 - Security Awareness Training (SAT),
 - Safety Survival Skills Training (SSST)
 - 2018 Information Security, Counterintelligence, Privacy Awareness, Records Management Refresher course from NIH (<http://irtsectraining.nih.gov/Default.aspx>)
 - Select the green “Enter Public Portal” button in the right-hand corner
 - Next select the red “Enter Public Training Portal” button
 - Select the correct course title to begin training
 - Provide the final training certificate with the following naming convention:
“NIH_SecurityA_and_PrivacyA_<LastName><FirstInitial>_YYYYMMDD

Status for all staff will be cleared or complete.

Credential	Status
Background Investigation	Cleared
Network Access	Cleared
SAT Date	Complete
Safety Survival Skills	Cleared

Ensure form 1137N for Personal Identification Verification (PIV)/Smartcard is sent to CDC security (<http://isp-v-maso-apps/EForms/download.aspx?ID=2026>) in order to get access to CDC networks, computers, and systems.

All federal employees working on the study will also need to meet the requirements above.

Continuous Maintenance of Staff

Rules of Behavior

Any updates to the Rules of Behavior document will require all staff to review and sign to ensure their access to study data is maintained. The DM Team will ensure all users who have access to the study data are provided the updated Rules of Behavior for their signature.

Out-Processing of Staff

Notification

Official out-processing should occur in People Processing (<https://peopleprocessing.cdc.gov/>) for users leaving CDC.

User System Access

If a user's role changes or if the user leaves the project or CDC, the data steward will review the data access spreadsheet. Appropriate actions (remove or change access for the user) will be taken by the PI and data steward and the spreadsheet updated.

Return of Equipment

The ATSDR program lead will ensure that all equipment is returned when a user leaves CDC or the project. Equipment will not be transferred to another center, division, etc. but will be returned to be securely erased (reimaged).

Procedures for Requesting Access to Data

The data steward of the study shall maintain a data access spreadsheet with the following information at a minimum (spreadsheet/location TBD):

- Date
- First Name
- Last Name
- Contractor/FTE
- CDC User ID
- Approved By
- Approved By Date
- Data Store (share, database, etc.)
- Data Set
- PII Indicator
- Role (data access level)
- Access Granted By
- Access Granted Date
- Access Removed By
- Access Removed Date

This spreadsheet will be stored in the *Raw Data* folder of the encrypted MUST share for this study. This folder will permit *Full* access to the PI/data steward and *Read* access for other users.

When a user requests access to data or changes the type of access to the data, a new entry will be added to this spreadsheet. PI and data steward must ensure that the user has signed the Rules of Behavior (ROB) for the study before the user is granted access to any study data.

Encrypted Multi-User Share Tool (MUST) Share

Share Location (URI)

[\\cdc.gov\locker\ATSDR_Camp_Lej_Can_Inc_Stu](https://cdc.gov/locker/ATSDR_Camp_Lej_Can_Inc_Stu)

User Roles

Admin (PI and data steward), General User (Contractors & FTE's validating, matching or analyzing data), Data Reader (Reviewers and anyone only needing read access)

Configuration of Shares

The encrypted MUST share will have the following folders: Admin, Raw Data, and Working.

Folders

Folder	Folder Description	Permissions
Admin (No Access)	Data or files used only by administrators	Admin (full), General User (no access), Data Reader (no access)
Raw Data (Read Only)	Data that needs to be preserved in its current form and not altered, and documents that will be modified only by the admin and viewed by other users such as the data access spreadsheet, PII Transfer spreadsheet, Manual of Procedures, and signed ROB.	Admin (full), General User (read), Data Reader (read)
Working (Read/Write)	Data that is being worked on by staff.	Admin (full), General User (read/write), Data Reader (read)

Role	Description
Admin	Principal investigators and those that will be administering permissions and encryption for the share.
General User	Users that will be working (analyzing, matching, linking, etc.) with the data.
Data Reader	Users that will only need to review the data but will not or should not be able to alter it.

The *Working* folder may have subfolders in it identified by the CDC user ID of each user working with data.

Shares are created and administered through the Multi-User Share Tool (MUST) at <http://itsotools.cdc.gov/must/>

The example shares listed below are all encrypted. To confirm a share is encrypted, look at the path name and specifically at the part after “\\cdc\”. If the next word is “locker”, then the share is encrypted at rest. If the next word is “project”, then the share is not encrypted at rest. All shares containing PII will be encrypted.

Multi-User Shares

Path	Description	MUST Group (automatically created by ITSO Tools)	Permissions (automatically assigned by ITSO Tool)	Role(s)
\\cdc\locker\<INVESTIGATION NAME>	Share Root	<INVESTIGATION NAME>-FC	Full Control (FC) – read, write	Admin
\\cdc\locker\<INVESTIGATION NAME>	Share Root	<INVESTIGATION NAME>-RO	Read Only (RO) - read	General User, Data Reader
\\cdc\locker\<INVESTIGATION NAME>\admin	Admin Subfolder	<INVESTIGATION NAME>.Admin-fc	Full Control (FC) – read, write	Admin

\\cdc\locker\<INVESTIGATION NAME>\admin	Admin Subfolder	<INVESTIGATION NAME>.Admin-ro	Read Only (RO) - read	None
\\cdc\locker\<INVESTIGATION NAME>\working	Working Subfolder	<INVESTIGATION NAME>.Working-fc	Full Control (FC) – read, write	Admin, General User
\\cdc\locker\<INVESTIGATION NAME>\working	Working Subfolder	<INVESTIGATION NAME>.Working-ro	Read Only (RO) - read	Data Reader
\\cdc\locker\<INVESTIGATION NAME>\raw_data	Raw_Data Subfolder	<INVESTIGATION NAME>.Raw_Data-fc	Full Control (FC) – read, write	Admin
\\cdc\locker\<INVESTIGATION NAME>\raw_data	Raw_Data Subfolder	<INVESTIGATION NAME>.Raw_Data-ro	Read Only (RO) - read	General User, Data Reader

Granting Access to Shares

The PI or data steward will grant users access to the MUST encrypted share using the MUST administration tool at <http://itsotools.cdc.gov/must/>

File Level Encryption

Any data containing PII that exists outside of SQL server must be encrypted at the file level using Symantec Encryption Desktop. Information about installing the software, configuring the encrypted share, or encrypting individual files can be found in the documents listed below, and the section of this manual entitled *Setting up Encryption Software – Local Laptop Folders and Share*:

- OCISO Installation Procedure for PGP Desktop 10.1.2
- OCISO Quick User Guide for PGP Desktop 10.1.2

Note: When the encrypted share is setup, the Project lead and data steward (at a minimum) will be configured as administrators. Anyone who needs to use the share will be configured as a user so that they can decrypt and encrypt files in the share. MUST share permissions will be used to limit what the user can access and modify.

Client Whole Disk Encryption

CDC laptops have whole disk encryption (MS BitLocker, Check Point, etc.) installed and enabled. CDC desktops do not have this software by default. A desktop will not ever be used for processing or storage of study PII. All staff who work with PII will have CDC laptops.

Requests to Move PII from Encrypted Share

Every effort will be made to keep data in the encrypted MUST share. If data needs to be moved from the share to another location, the move must be approved by the PI and logged in a PII Transfer spreadsheet. The PI and Data steward are responsible for maintaining this spreadsheet. The spreadsheet will contain the following information at a minimum (spreadsheet/location TBD):

- Date
- First Name
- Last Name
- Contractor/FTE
- CDC User ID
- Approved By
- Approved By Date
- Data Set
- PII Indicator
- Data Transferred To (Laptop Name, System Name, etc.)
- Purpose
- Data Deleted By
- Data Deleted Date
- Notes (Describe how data was deleted)

This spreadsheet should be stored in the *Raw Data* folder of the encrypted MUST share for this study.

Securely Receiving/Sending Data

Use CDC's Secure Access Management System Secure Data Exchange (SAMS SDX) electronic authentication level 3 to electronically send or receive PII. <https://sams.cdc.gov> Use of systems or methods, other than SAMS, to electronically send or receive PII must be approved in writing by the NCEH/ATSDR Information Systems Security Officer (ISSO) prior to its use.

Data Disclosures

Disclosure of PII to entities outside of CDC (e.g., cancer registries, credit bureaus, etc.) must be approved by the PI and logged in a spreadsheet. The spreadsheet should contain the following information at a minimum:

- Date
- Entity Data Disclosed To
- Entity POC Name
- Entity POC Email
- Entity POC Phone Number
- Approved By
- Approved By Date
- Data Set
- PII Indicator
- Disclosure Purpose
- Data Disclosed By
- Data Disclosed Date
- Data Transfer Method
- Approved by ISSO
- ISSO Approval Date
- Notes

At the end of the investigation, before leaving the field, the data must be transferred to the requesting health agency and wiped from the CDC devices. Upon return to CDC, an ITSO ticket to do a complete wipe of the computer should be submitted. The requesting agency will then be advised that disclosures should not be made without a fully executed data use agreement (DUA).

This spreadsheet will be stored in the *Raw Data* folder of the encrypted MUST share for this study.

Before the final transfer of data to the requesting agency is made ISSO will determine that adequate controls exist to protect the data in transit. Written approval (usually via email) will be maintained in the *Raw Data* folder of the encrypted MUST share for the study. Approval will also be noted in the disclosure spreadsheet.

Transfer of data

PII data will not need to be transferred to entities outside of the CDC environment until the final closing of the investigation before leaving the field it will be returned to the requesting health agency and logged as a Data Disclosure. Data from all laptops will be merged nightly into a production database on a single laptop and exports from the production database nightly will be performed by the DM Team. Extracts will be stored in the encrypted *Working* folder. Data will be wiped from all other CDC laptops nightly. Data that will be transferred outside of the SQL Server Environment will be in flat file format with Symantec Encryption (PGP) applied to the file and a log of all data extractions will be maintained by the DM Team Lead to ensure proper accounting of all data exports. Each file that is exported will be tested by a second DM Team member to ensure the PGP encryption is applied correctly. Prior to adding encrypted flat files to the SAMS Network (or other ISSO approved file transfer mechanism) approval to transfer the file will be obtained as noted in "Requests to move PII from Encrypted Share". For all data transfers the following is applicable:

- Data will not be transferred outside of the CDC laptops during the investigation.
- Data will be backed up on the MUST server nightly. Columns containing any identifiers (including address) will be encrypted.
- The final, concatenated deliverable dataset will be provided to the state or local requesting health agency

Assessment of Chemical Exposures (ACE) Investigations Data Flow Diagram

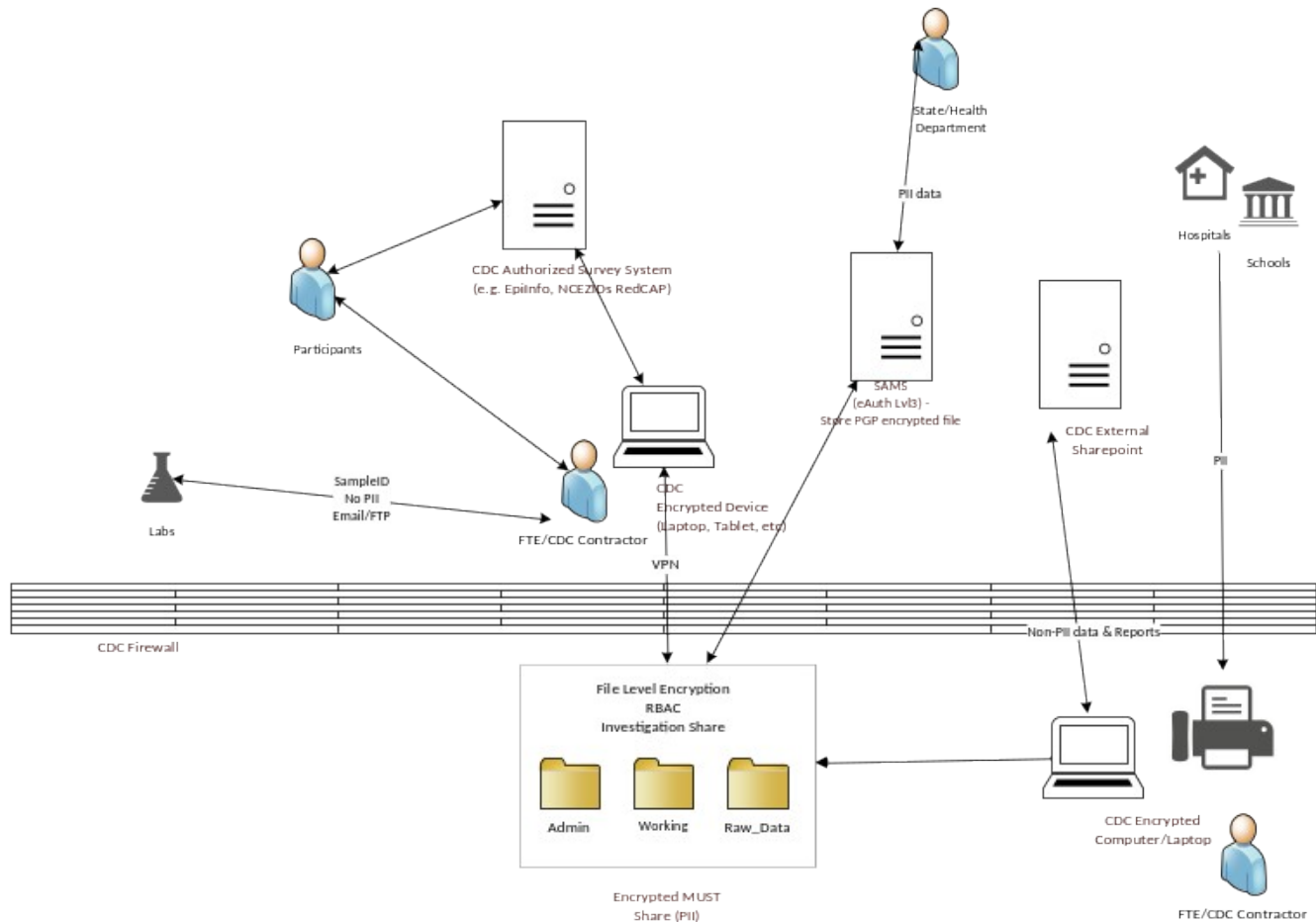


Figure 1: Data Flow Diagram outlines the flow of encrypted data to these entities

CDC Environment

The CDC Environment will consist of:

- Role Based Access Control (RBAC) folder with file level encryption (PGP or similar)

Prior to data transfer to requesting health agency:

- Give project lead and data steward notification to review and approve the encrypted file(s) for transfer.
- Logging of destination, recipient, and encryption keys (encryption key tracking to be maintained separately from recipient tracking) by PI or data steward in a tracking spreadsheet.

De-identification of Data

De-identified, analysis-ready datasets will be exported from the SQL Server database in the format required for analysis. These data will exclude columns identified as PII (SSN, Name, Dates) as documented in the SQL Server schema documentation but could contain data by limited-use columns (e.g., race, sex) for analysis purposes if it is determined that these columns alone would not identify any cohort members.

Privacy

Background

The study is a Privacy Act system covered by System of Records Notice (SORN) 09-19-0001 Records of Persons Exposed or Potentially Exposed to Toxic or Hazardous Substances, HHS/ATSDR (<https://www.federalregister.gov/documents/2011/01/25/2010-33004/privacy-act-of-1974-report-of-modified-or-altered-system-of-records>)

Inquiries

Any inquiries from individuals related to their PII in this study will be referred back to the requesting health agency. If an individual is concerned that his/her PII has been used inappropriately and communicates that to the CDC, the project lead will evaluate the concern and report the incident to the CDC Chief Privacy Officer within 48 hours.

Setting up Encryption Software – Local Laptop Folders and Share

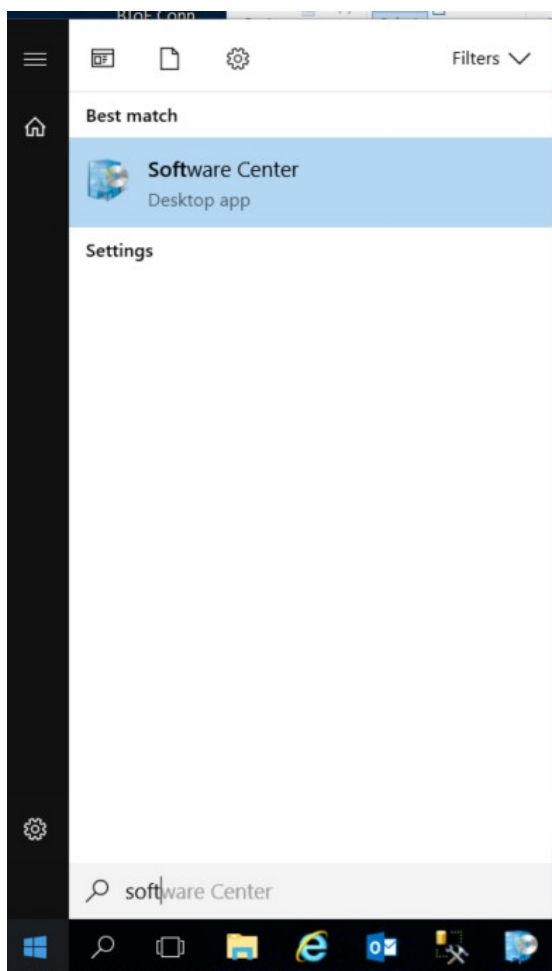
Symantec Encryption (PGP) Software Install Additional Help

To start the install, do the following steps:

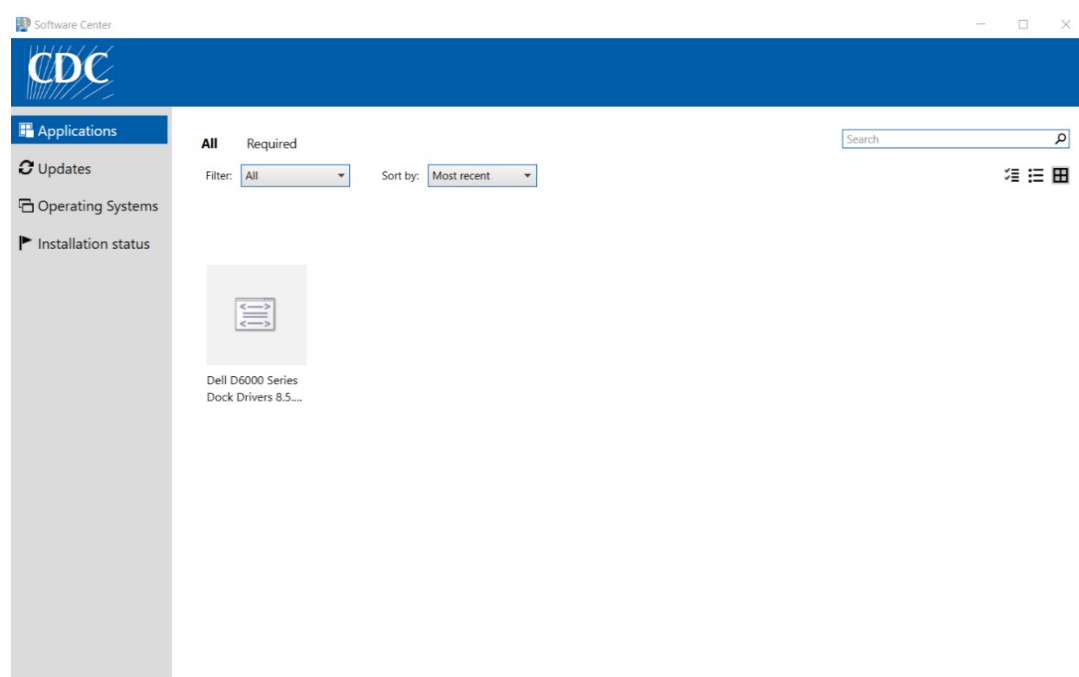
1. Click on the Windows start button



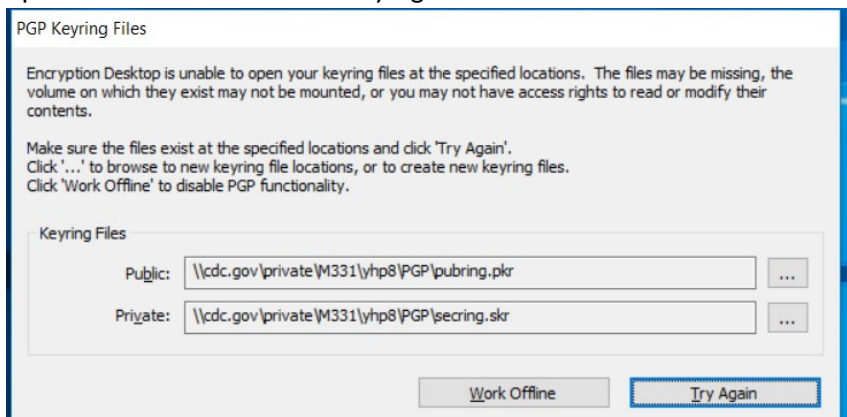
2. Start typing software center – this should bring up the Software Center Desktop App



3. The app should look something like this: (PGP is not shown as it's already installed)



4. If PGP is displayed, click on it and it will display the Application details along with the *Install* button.
5. If it is not displayed, leave the laptop on and connected to VPN overnight, if possible.
6. Click on *Install* and it will change the status from *Available* to *Downloading* with a percentage of completion.
7. Once installed, restart your laptop.
8. Sign back into your laptop via Smartcard.
9. Once you are back at the desktop location on your laptop, you may get prompted with keyring files with options to “Work Offline” or Try Again”.



10. Before clicking any option, sign into VPN.
11. Click on the “...” button to browse and select the option at the bottom of the window to use the default location on the local laptop.
12. Create the public and private keyring files in the default location on the laptop.
13. Once created, click “Try Again” and it should go through.
14. Follow the rest of the PGP Installation Guide.

How to Test Encryption on Local Laptops

The overall process to test encryption is as follows:

- **Conditions:** Setup share and folder permissions for testers, but don’t grant them ability to decrypt data.
- **Test:** Have users go to share and report what they find there. Have users try to write a file to the root of the share and report results.
- **Success Criteria:** Testers should have access to the share. They should not be able to write files to the root of the share. The files and folders should appear encrypted to the testers.

Each user will be required to test the performance of their PGP software on their CDC-issued laptop prior to accessing the PII data.

Shredding of Electronic Files Using Encryption

Upon completion of work with PII data files, the files will be destroyed using the File Shredder application included with the PGP Software. Instructions on the use of the PGP shredder can be found on page 23 of the “OCISO PGP Quick User Guide.pdf” document.

Incident Response

Incidents involving the study data or systems storing, processing or transmitting this data must be reported to the CDC Computer Security Incident Response Team within 1 hour of learning about the incident. Definitions of an incident can be found in the CDC Security Awareness Training (SAT) and in the references below.

Computer Security Incident Response Team (CSIRT)

Email: csirt@cdc.gov

Phone: 866-655-2245

References

Computer Security Incident Response: Host Isolation, Removal, and Mitigation (CDC-IS-2009-01)

CDC Information Security Enterprise Incident Response Plan Version 5.2

Email Usage and Web Browsing

Users that are processing study data that contains PII will not browse the web or check email on their computer/laptop. Instead, users should use citgo.cdc.gov for these activities to limit connectivity while processing PII data.

References/Associated Documents

Document Name	Description	Location
OCISO PGP Installation Procedure	Installation Procedure manual for PGP Desktop 10.1.2	ACE SharePoint folder "PGP Encryption"
OCISO PGP Quick User Guide	Quick User Guide to get PGP set up for use after installation	ACE SharePoint folder "PGP Encryption"
PGP Encryption – Troubleshooting Keys	Step-by-step guide on how to clear your cached PGP Encryption Key	ACE Documents SharePoint folder "PGP Encryption"
PGP Encryption – How to Encrypt a folder	Step-by-step guide on how to create and encrypt your C:\CIS encrypted folder on your local laptop.	ACE Documents SharePoint folder "PGP Encryption"
ACE Rules of Behavior	States the Rules of Behavior for the Appropriate Use of Data	Camp Lejeune Working Documents SharePoint folder "Rules of Behavior"
MUST Share Encryption Limitations	E-mail regarding the error with PGP and steps with encryption	ACE Working Documents SharePoint root folder