Encryption/Decryption of Identifiable Data Written to Foreign Media

Any identifiable data being sent from the CMS mailroom on foreign media must be encrypted. DESY has implemented the encryption of identifiable data to foreign media in their Release V6.3.1.

When the DUA selected for a DESY request indicates that identifiable data will be shipped on foreign media, the DESY Requestor will be prompted as to whether they want the data encrypted using PKWare, IBM z/OS, or whether they want the data written to a mainframe file that can be downloaded and encrypted on the Requestor's desktop using Pointsec encryption software. The Requestor should know which software the data Recipient will be using when the DESY request is made.

PKWare is the mainframe secure zip software that is being provided free of charge to recipients of CMS data on foreign media. Unless the data Recipient has purchased the necessary software/hardware to decrypt files using IBM z/OS software or you know that you will be downloading the data and encrypting it on your desktop, the DESY Requestor should use PKWare to encrypt files via DESY.

The decryption software for files that have been encrypted using PKWARE can be found at the following URL:

http://securezippartner.pkware.com/

The Sponsor ID is '7708' and the Sponsor Name is 'CMS'. This information should be conveyed to the data Recipient. ** ***Only users outside of CMS should be registering on the PKWare website and downloading the decryption software.***

Users will also need a Sponsor Distribution Package (SDP) from CMS, which contains a public certificate for the Agency. The SDP is a Binary File/Key that is needed to complete the installation of the SecureZIP Partner software. To obtain the SDP file, please email your request to:
John.Suchocki@cms.hhs.gov and Mark.Zeller@cms.hhs.gov

Contact information for PKWare support is as follows:

Normal Business Hours (8:00am – 6:00pm CST)
Phone: 1-937-847-2687
Email: partnersupport@pkware.com

24x7 Priority Support
Phone: 1-937-847-6149

If PKWare or IBM z/OS software is selected, DESY will automatically generate a password for decryption, and password will be emailed to the data Recipient when the data is shipped. It is important that the data Recipient's email address in the DADSS' Data Use Agreement is accurate.

If the data Recipient loses the password required to decrypt the file, please email desy_support@cms.hhs.gov, and include the DESY request number of the file for which you are requesting the password. One of the DESY System Administrators will be able to have the password resent to the recipient.

The LRECL and BLKSIZE for files generated from DESY may be required for your decryption routine:

	LRECL		BLKSIZE	
NCH & SAF	13054	VB	32760	(All output formats.)
FINDER FILE VIEW	14	FB	32760	
MEDPAR	886	FB	31896	
DENOMINATOR	140	FB	32760	
NAME & ADDRESS	248	FB	32736	
VITAL STATS	248	FB	32736	
XREF & Converts	30	FB	27990	